

目 录

第 1 章 通用命令	10
1.1 模式命令	10
1.1.1 configure terminal	10
1.1.2 disable	10
1.1.3 enable.....	11
1.1.4 exit.....	11
1.2 文件管理命令	12
1.2.1 copy running-config startup-config.....	12
1.2.2 delete startup-config	12
1.2.3 download configure.....	12
1.2.4 download union	13
1.2.5 upload configure.....	13
1.2.6 write.....	14
1.3 系统管理命令	14
1.3.1 access-class	14
1.3.2 disable telnet	15
1.3.3 enable telnet	15
1.3.4 enable password.....	16
1.3.5 exec-timeout	16
1.3.6 hostname	17
1.3.7 password.....	17
1.3.8 reset	18
1.3.9 reset mod ule.....	18
1.3.10 reset system	18
1.3.11 set datetime.....	19
1.3.12 show datetime.....	19
1.3.13 show history	20
1.3.14 show system	20
1.3.15 show version.....	21
1.3.16 terminal	21
1.3.17 who	22
1.4 查看配置命令	22
1.4.1 show running-config	22

1.4.2 show startup-config.....	23
1.5 Mac 地址表命令	23
1.5.1 bridge ageing-time	23
1.6 网络调试命令	24
1.6.1 ping.....	24
1.6.2 trace-route.....	25
第 2 章 模块管理命令.....	26
2.1 模块配置命令	26
2.1.1 create module.....	26
2.1.2 remove module.....	26
2.2 模块查看命令	27
2.2.1 show bdver.....	27
2.2.2 show module.....	27
第 3 章 端口命令	29
3.1 端口通用配置	29
3.1.1 interface.....	29
3.1.2 bandwidth.....	29
3.1.3 description	30
3.1.4 duplex	30
3.1.5 flowcontrol.....	31
3.1.6 show flowcontrol.....	31
3.1.7 show interface.....	32
3.1.8 shutdown.....	33
3.2 MIRROR 命令	33
3.2.1 mirror.....	33
3.2.2 show mirror.....	34
3.3 端口限速命令	34
3.3.1 portrate	34
3.3.2 show portrate.....	35
3.4 广播风暴控制命令	35
3.4.1 storm -control.....	35
3.4.2 show storm-control.....	36
第 4 章 vlan 命令	37
4.1 vlan 创建命令	37
4.1.1 vlan database.....	37
4.1.2 Vlan	37

4.2 vlan 端口配置命令	38
4.2.1 switchport access	38
4.2.2 switchport hybrid allowed vlan add	38
4.2.3 switchport hybrid allowed vlan all	39
4.2.4 switchport hybrid allowed vlan none	40
4.2.5 switchport hybrid allowed vlan remove	40
4.2.6 switchport hybrid vlan	41
4.2.7 switchport mode	41
4.2.8 switchport trunk allowed vlan add	42
4.2.9 switchport trunk allowed vlan all	43
4.2.10 switchport trunk allowed vlan none	43
4.2.11 switchport trunk allowed vlan remove	44
4.3 vlan 查看命令	44
4.3.1 show vlan	44
4.3.2 show interface switchport	45
第 5 章 MSTP 命令	46
5.1 MSTP 配置命令	46
5.1.1 spanning-tree mst cisco-interoperability	46
5.1.2 spanning-tree mst configuration	46
5.1.3 spanning-tree mst enable	47
5.1.4 spanning-tree mst errdisable-timeout	47
5.1.5 spanning-tree mst forward-time	48
5.1.6 spanning-tree mst hello-time	48
5.1.7 spanning-tree mst max-age	49
5.1.8 spanning-tree mst max-hops	49
5.1.9 spanning-tree mst portfast	50
5.1.10 spanning-tree mst portfast bpdu-filter	50
5.1.11 spanning-tree mst portfast bpdu-guard	51
5.1.12 spanning-tree mst priority	51
5.1.13 instance	52
5.1.14 region	53
5.1.15 revision	53
5.1.16 spanning-tree mst force-version	53
5.1.17 spanning-tree mst guard root	54
5.1.18 spanning-tree mst instance	54
5.1.19 spanning-tree mst link-type	55
5.1.20 spanning-tree mst pathcost	56

5.1.21 spanning-tree mst priority.....	57
5.1.22 clear spanning-tree detected protocols.....	58
5.2 MSTP 查看命令.....	58
5.2.1 show spanning-tree mst.....	58
5.3 MSTP 调试命令.....	60
5.3.1 debug mstp.....	60
5.3.2 debug mstp all.....	60
5.3.3 debug mstp cli.....	61
5.3.4 debug mstp packet.....	61
5.3.5 debug mstp protocol.....	62
5.3.6 debug mstp timer.....	62
第 6 章 IGMP SNOOPING 命令.....	64
6.1 IGMP SNOOPING 配置命令.....	64
6.1.1 ip igmp snooping.....	64
6.1.2 ip igmp snooping fast-leave.....	64
6.1.3 ip igmp snooping fast-leave-timeout.....	65
6.1.4 ip igmp snooping group-membership-timeout.....	65
6.1.5 ip igmp snooping mrouter.....	66
6.1.6 ip igmp snooping query-membership-timeout.....	66
6.1.7 ip ip igmp snooping vlan.....	67
6.2 IGMP SNOOPING 查看命令.....	67
6.2.1 show ip igmp snooping.....	67
6.2.2 show ip igmp snooping age-table.....	68
6.2.3 show ip igmp snooping mrouter.....	69
6.2.4 show ip igmpv2.....	69
6.3 IGMP SNOOPING 调试命令.....	70
6.3.1 debug igmp snooping.....	70
第 7 章 ACL 命令.....	72
7.1 ACL 配置命令.....	72
7.1.1 基于标准 IP 的 ACL 规则.....	72
7.1.2 基于扩展 IP 的 ACL 规则.....	73
7.1.3 字符类型的 ACL 规则.....	74
7.1.4 access-group.....	75
7.2 ACL 查看命令.....	75
7.2.1 show access-group.....	75
7.2.2 show access-list.....	76

第 8 章 IP 路由命令	77
8.1 配置命令	77
8.1.1 arp	77
8.1.2 arp lock	77
8.1.3 arp static	78
8.1.4 show arp	78
8.1.5 ip prefix-list	79
8.1.6 ip route	80
8.1.7 match interface	81
8.1.8 match ip	81
8.1.9 match metric	82
8.1.10 match routetype	82
8.1.11 match tag	83
8.1.12 router-id	83
8.1.13 routemap	84
8.1.14 set ip	85
8.1.15 set metric	85
8.1.16 set metric-type	86
8.1.17 set tag	86
8.2 显示命令	87
8.2.1 show ip prefix-list	87
8.2.2 show ip route	87
8.2.3 show ip route connected	89
8.2.4 show ip route database	90
8.2.5 show routemap	91
第 9 章 RIP 命令	92
9.1 配置命令	92
9.1.1 default-information originate	92
9.1.2 default-metric	92
9.1.3 distance	93
9.1.4 distribute-list	93
9.1.5 ip rip authentication	94
9.1.6 ip rip metric	95
9.1.7 ip rip receive version	95
9.1.8 ip rip receive -packet	96
9.1.9 ip rip send version	96
9.1.10 ip rip send -packet	97

9.1.11 ip rip split-horizon.....	97
9.1.12 maximum-prefix	98
9.1.13 neighbor	98
9.1.14 network	99
9.1.15 offset-list	99
9.1.16 passive-interface	100
9.1.17 recv-buffer-size.....	101
9.1.18 redistribute	101
9.1.19 route.....	102
9.1.20 router rip.....	102
9.1.21 timers	103
9.1.22 version	103
9.2 查看命令	104
9.2.1 show ip rip.....	104
9.2.2 show ip route rip.....	105
9.2.3 show running rip.....	106
9.3 调试命令	106
9.3.1 debug rip.....	106
9.3.2 debug rip all.....	107
9.3.3 debug rip events.....	107
9.3.4 debug rip packet.....	108
第 10 章 OSPF 命令	109
10.1 配置命令	109
10.1.1 area authentication	109
10.1.2 area default-cost	109
10.1.3 area filter-list.....	110
10.1.4 area nssa.....	111
10.1.5 area range.....	112
10.1.6 area shortcut	112
10.1.7 area stub	113
10.1.8 area virtual-link.....	113
10.1.9 area virtual-link authentication	114
10.1.10 auto-cost reference-bandwidth.....	115
10.1.11 compatible rfc1583.....	116
10.1.12 default-information originate	116
10.1.13 default-metric	117
10.1.14 distance	117

10.1.15 distribute-list	118
10.1.16 host	119
10.1.17 ip ospf authentication	119
10.1.18 ip ospf authentication-key	120
10.1.19 ip ospf cost	120
10.1.20 ip ospf database-filter	121
10.1.21 ip ospf dead-interval	121
10.1.22 ip ospf disable all	122
10.1.23 ip ospf hello-interval	122
10.1.24 ip ospf message-digest-key	123
10.1.25 ip ospf mtu	123
10.1.26 ip ospf mtu-ignore	124
10.1.27 ip ospf network	124
10.1.28 ip ospf priority	125
10.1.29 ip ospf retransmit-interval	126
10.1.30 ip ospf transmit-delay	126
10.1.31 max-concurrent-dd	127
10.1.32 neighbor	127
10.1.33 network	128
10.1.34 passive-interface	128
10.1.35 redistribute	129
10.1.36 router ospf	130
10.1.37 router-id	130
10.1.38 summary-address	131
10.1.39 timers spf	131
10.2 查看命令	132
10.2.1 show ip ospf	132
10.2.2 show ip ospf database	133
10.2.3 show ip ospf interface	135
10.2.4 show ip ospf neighbor	136
10.2.5 show ip ospf route	137
10.2.6 show ip ospf virtual-links	137
10.2.7 show running ospf	138
10.3 调试命令	139
10.3.1 debug ospf	139
10.3.2 debug ospf all	139
10.3.3 debug ospf events	140

10.3.4 debug ospf ifsm	141
10.3.5 debug ospf lsa.....	141
10.3.6 debug ospf nfsm.....	142
10.3.7 debug ospf packet	142
10.3.8 debug ospf route	143
第 11 章 VRRP 命令	144
11.1 配置命令	144
11.1.1 disable/enable.....	144
11.1.2 router vrrp.....	144
11.1.3 vrrp ip-address.....	145
11.1.4 vrrp advertisement-interval	146
11.1.5 vrrp authentication.....	146
11.1.6 vrrp preempt	147
11.1.7 vrrp priority	147
11.2 查看命令	148
11.2.1 show vrrp.....	148
11.3 调试命令	149
11.3.1 debug vrrp.....	149
11.3.2 debug vrrp all	149
11.3.3 debug vrrp events	150
11.3.4 debug vrrp packet	150
第 12 章 DHCP-RELAY 命令	152
12.1 配置命令	152
12.1.1 dhcp relay	152
12.1.2 dhcp server	152
12.2 查看命令	153
12.2.1 show debugging dhcp-relay	153
12.3 调试命令	154
12.3.1 debug dhcp-relay	154
12.3.2 debug dhcp-relay all	154
12.3.3 debug dhcp-relay events	155
12.3.4 debug dhcp-relay packet	155
第 13 章 系统日志命令	157
13.1 通用日志命令	157
13.1.1 debug ip	157
13.1.2 log display	158

13.1.3 no debug all158

13.1.4 show debugging158

13.1.5 show log160

13.1.6 show log display161

第 1 章 通用命令

1.1 模式命令

1.1.1 configure terminal

命令

configure terminal

模式

特权模式

参数

无。

描述

configure terminal命令用来进入配置模式

举例

#进入全局配置模式:

Switch#configure terminal

Switch(config)#

1.1.2 disable

命令

disable

模式

特权模式

参数

无

描述

disable命令用来关闭特权模式，退回到普通模式。

举例

#关闭并退回到普通模式:

Switch#disable

Switch>

1.1.3 enable

命令

enable

模式

普通模式

参数

无

描述

如果密码通过，进入特权模式。

举例

#从普通模式进入特权模式：

Switch> enable

password:*****

switch#

1.1.4 exit

命令

exit

模式

所有模式

参数

无

描述

exit命令用来结束当前模式，回到前一个模式。

举例

#从特权模式退回到普通模式：

Switch#exit

Switch>

1.2 文件管理命令

1.2.1 copy running-config startup-config

命令

copy running-config startup-config

模式

特权模式

参数

无。

描述

copy running-config startup-config 命令将系统当前配置保存为启动配置文件。

举例

无。

1.2.2 delete startup-config

命令

delete startup-config

模式

特权模式

参数

无。

描述

删除启动配置文件。执行该命令后重启交换机，将恢复到出厂设置。

举例

无。

1.2.3 download configure

命令

download configure <ip-address> <file-name>

模式

特权模式

参数

ip-address : TFTP 服务器ip地址。

file-name: TFTP服务器上的配置文件名。

描述

从 TFTP 服务器上将配置文件下载到交换机作为启动配置文件，重启交换机后下载的配置文件生效。

举例

#将配置文件下载到主机 172.16.0.1.文件名为 conf.txt:

Switch#download configure 172.16.0.1 conf.txt

1.2.4 download union

命令

download union <ip-address> <file-name>

模式

特权模式

参数

ip-address: TFTP 服务器ip地址。

file-name : TFTP 服务器上的联合文件名。

描述

下载联合文件。联合文件包含主控与线卡的 image 文件和版本文件。联合文件下载到主控中后，会检查主控和线卡的 image 文件版本，若版本不一致则将其更新为下载的版本，并修改版本文件。

举例

#从主机 172.16.0.200 下载联合文件到交换机:

Switch#download union 172.16.0.200 iSpirit12804_1v02.uni

1.2.5 upload configure

命令

upload configure <ip-address> <file-name>

模式

特权模式

参数

ip-address: 表示文件上传的目的TFTP 服务器的IP 地址。

file-name : 保存到 TFTP 服务器上的配置文件名。

描述

将交换机的启动配置文件保存到 TFTP 服务器上。

举例

#将启动配置文件保存到主机 172.16.0.200 上，命名为 conf：

```
Switch#upload configure 172.16.0.200 conf
```

1.2.6 write

命令

write

模式

特权模式。

参数

无。

描述

保存当前用户配置的设置信息。

举例

无。

1.3 系统管理命令

1.3.1 access-class

命令

access-class <list-name>

no access-class [<list-name>]

模式

终端配置模式

参数

list-name: 访问列表的名字(数字名或字符串名)。

描述

access-class 命令通过调用一条基于 IP 的访问控制列表,实现对用户的控制。

no access-class 命令删除对用户的访问控制配置。

举例

#调用名为 lenovo 12800 的访问控制列表规律用户:

Switch(config-line)#no access-class lenovo 12800

Switch(config-line)#

1.3.2 disable telnet

命令

disable telnet

模式

终端配置模式。

参数

无。

描述

关闭 telnet 服务功能,用户不能 telnet 到设备。

举例

无。

1.3.3 enable telnet

命令

enable telnet

模式

终端配置模式。

参数

无。

描述

打开 telnet 服务功能,用户可以 telnet 到设备。默认打开。

举例

无。

1.3.4 enable password

命令

enable password <password>
no enable password

模式

全局配置模式

参数

password : 密码字符串。缺省密码为空。

描述

enable password 命令用来修改交换机从普通模式进入特权模式的密码。
no enable password 命令用来取消密码。

举例

#修改交换机的密码为admin :
Switch(config)#enable password admin

1.3.5 exec-timeout

命令

exec-timeout <minutes> <seconds>
no exec-timeout

模式

终端配置模式

参数

minutes : 分钟, 范围 0-35791。
seconds : 秒, 范围 0-2147483。

描述

exec-timeout 命令用来配置 telnet 终端空闲超时时间。默认值 10 分钟。
no exec-timeout 命令用来取消配置, 恢复默认值。

举例

#配置超时时间为 15 分钟 :
Switch(config-line)#exec-timeout 15

Switch(config-line)#

1.3.6 hostname

命令

hostname <name>

no hostname

模式

全局配置模式。

参数

name: 系统的名字，要以字母开头。默认的系统名为 Switch。

描述

hostname 命令用来修改系统的名字。

no hostname 将系统名字恢复为出厂设置。

举例

#将系统名改为 i12804：

Switch(config)#hostname i12804

i12804(config)#

1.3.7 password

命令

password <password>

no password

模式

全局配置模式。

参数

password: 密码字符串。默认没有密码。

描述

password 命令用来设置 Telnet 连接密码。

no password 命令用来取消密码设置，恢复默认值。

举例

无。

1.3.8 reset

命令

reset

模式

特权模式。

参数

无。

描述

reset 命令用来重启交换机主控模块。

举例

无。

1.3.9 reset module

命令

reset module [<Module-id>])

模式

特权模式

参数

module: 重启模块。

module-id : 线卡编号，对于 12804 范围：1-4，12810 范围：1-8。

描述

reset module 命令用来重启交换机或指定的模块。

举例

#重启第一槽的模块：

Switch#reset module 1

1.3.10 reset system

命令

reset system

模式

特权模式。

参数

无。

描述

reset system 命令用来重启交换机所有模块。

举例

无。

1.3.11 set date -time

命令

set datetime <year> <month> <day> <hour> <minute> <second>

模式

特权模式

参数

year: 设置年，范围：2000-2050。

month: 设置月，范围：1-12。

day: 设置日，范围：1-31。

hour: 设置小时，范围：0-23。

minute: 设置分钟，范围：0-59。

second: 设置秒，范围：0-59。

描述

set datetime 命令用来设置系统时间。

举例

无。

1.3.12 show date -time

命令

show date-time

模式

普通模式/特权模式

参数

无

描述

show date-time 命令用来显示系统当前日期和时间

举例

无。

1.3.13 show history

命令

show history

模式

普通模式/特权模式。

参数

无。

描述

show history 命令用来显示命令历史 ,可以显示本命令之前执行的 20 条命令。

举例

无。

1.3.14 show system

命令

show system

模式

普通模式/特权模式

参数

无

描述

show system 命令用来显示系统运行时间。

举例

#显示系统运行时间：

Switch#show system

System Up Time : 0-Days 0-Hours 59-Minutes 45-Seconds

Switch#

1.3.15 show version

命令

show version

模式

普通模式/特权模式

参数

无

描述

show version 命令用来显示系统 image 文件版本信息。

举例

#显示系统版本

Switch>show version

iSpirit12804 1.0.2

Build time:Apr 29 2006, 16:35:19

Switch>

1.3.16 terminal

命令

terminal{length <number>|no length}

模式

普通模式/特权模式

参数

length: 指定每次显示到屏幕的行数。默认25行。

no length: 取消显示行数的设置。

描述

terminal 命令用来配置终端一次显示到屏幕的行数。

举例

#配置终端每次显示10行:

Switch>terminal length 10

1.3.17 who

命令

who

模式

普通模式/特权模式

参数

无

描述

who 命令用来显示当前 vty 的用户。

举例

#显示当前的VTY用户：

Switch#who

vty[0] connected from

1.4 查看配置命令

1.4.1 show running-config

命令

show running-config [access-list | interface | ip {igmp snooping | route} |
key chain | mstp | ospf | prefix-list | rip | route-map | vlan]

模式

特权模式

参数

access-list: ACL的相关配置。

interface: 接口的相关配置，包括物理接口和虚拟接口。

ip igmp snooping : igmp snooping的相关配置。

ip route: 路由的相关配置。

key chain: 认证密钥链的相关配置。

mstp: mstp的相关配置。

ospf : osp的相关配置。

prefix-list : 前缀列表的相关配置。

rip: rip协议的相关配置。

route-map: 路由表的相关配置。

vlan : vlan 的相关配置。

描述

show running-config 命令用来显示当前的配置信息。

举例

无。

1.4.2 show startup-config

命令

show startup-config

模式

特权模式

参数

无

描述

show startup-config 命令用来显示系统启动配置文件内容。

举例

无。

1.5 Mac 地址表命令

1.5.1 bridge ageing-time

命令

bridge ageing-time <time>

no bridge ageing-time

模式

全局配置模式

参数

time : mac 表老化时间，范围：10-1000000 秒。默认 300 秒。

描述

bridge ageing-time 命令用来设置 mac 地址表的老化时间。

no bridge ageing-time 命令将 mac 地址表的 age 时间恢复出厂值。

举例

#设置交换机的老化时间为100 秒：

```
Switch(config)#bridge ageingtime 100
```

```
Switch(config)#
```

1.6 网络调试命令

1.6.1 ping

命令

```
ping <ip-address> [n <count> | -l <size> | -r <count> | -s <count> | -j  
<count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*
```

模式

特权模式

参数

ip-address: 目标IP 地址。

-n: 发送请求的数目。

-l: 发送包长度。

-r: 记录指定跳数的路由。

-s: 记录指定跳数的时间。

-j: 源带松散路由，输入路由跳数和相关跳的IP 地址。可以重复输入多个IP 地址。

-k: 源带严格路由，输入路由跳数和相关跳的IP 地址。可以重复输入多个IP 地址。

-w: 等待每个回应的超时时间，单位秒。

描述

ping 是一个测试另一台主机是否可达的网络调试工具。简单的应用只要输入目标主机的IP地址就可以了；如果使用ping作为诊断工具，可以输入更详细的参数。

举例

#向主机172.16.0.1发5个请求包。


```
Switch#ping 172.16.0.1 -n 5
```

1.6.2 trace-route

命令

```
trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* |  
-w <timeout>]*
```

模式

特权模式

参数

ip-address: 目标IP 地址。

-h: 最大跳数。

-j: 源带松散路由，输入路由跳数和相关跳的IP 地址。 可以重复输入多个IP 地址。

-w: 超时时间(秒)。

描述

tracert可以检测数据包从一台主机传到另一台主机所经过的路由。

如果只是要实现这个功能，用户只需要输入目标IP 地址就可以了。如果要作为网络诊断可以输入相关参数。

Tracert 的实现方式是这样的，从本主机向目的主机发送TTL递增的UDP数据包。如果TTL 为零，经过的路由器会发送TTL 耗尽，主机不可达的ICMP 包；如果到达主机但是主机没有该UDP包的端口，主机就会回应端口不可达的ICMP包。tracert根据所经过的响应的ICMP包是主机不可达还是端口不可达来判断是否到达目的主机。如果是主机不可达说明经过的是路由器，打印这个路由器的IP地址，继续发送TTL 加1 的UDP包，直到TTL 等于Maximum time to live。如果是端口不可达说明到达了目的主机，打印这个主机的IP 地址，停止发送UDP包。

举例

#检测目的为192.168.10.2，最大跳数10跳的所经路由：

```
Switch#trace -route 192.168.10.2 -n 10
```

第 2 章 模块管理命令

2.1 模块配置命令

2.1.1 create module

命令

```
creat module {<module-id>}{<module-type>}
```

模式

模块配置模式

参数

module-id: 线卡编号，对于12804范围：1-4，12810范围：1-8。

module-type: 模块类型，包括：24gt、24gx、16xt、28xt、10g2x。

描述

creat module 命令用来创建线卡。该命令可在空槽位创建一个虚拟的线卡，并可进行端口配置。当该槽位插入类型相符的线卡时，之前的配置会下发到线卡并生效。当该槽位插入类型不相符的线卡时，主控终端会提示线卡类型不符，需删除该线卡，然后交换机会自动创建线卡。

举例

#在2号槽位创建24gx：

```
Switch(config-module)#create module 2 24gx
```

2.1.2 remove module

命令

```
remove module {<module-id>}{<module-type>}
```

模式

模块配置模式

参数

module-id: 线卡编号，对于12804范围：1-4，12810范围：1-8。

module-type: 模块类型，包括：24gt、24gx、16xt、28xt、10g2x。

描述

remove module 命令用来删除线卡。若该槽位有线卡，则删除后会再自动创建线卡。

举例

#删除第二槽的线卡：

Switch(config-module)#remove module 2

2.2 模块查看命令

2.2.1 show bdver

命令

show bdver <module-id>

模式

特权模式

参数

module-id: 模块号，主控编号为 17-18，12804 线卡编号为 1-4，12810 线卡编号为 1-8。

卡编

描述

show bdver 命令用来显示模块的 image 文件版本。

举例

#Switch#sh bdver

slotid	modulename	ver
1	24gt	1.0.2
2	24gx	1.0.2
3	10g2x	1.0.2
4	null	0.0.0
17	mgt-a	1.0.2
18	mgt-b	0.0.0

2.2.2 show module

命令

show module [<Module-id>]

模式

特权模式

参数

Module-id：模块号。12804 线卡编号为 1-4，12810 线卡编号为 1-8，主控编号为 17-18，电源编号为 19-21，风扇编号为 22。

描述

show module 命令用来显示模块类型和状态。

举例

#显示当前的模块类型和状态

Switch#show module

slotid	modulename	online	other
1	24gt	online	on /heartbeat
2	null	offline	off/no heartbeat
3	null	offline	off/no heartbeat
4	null	offline	off/no heartbeat
17	mgt -a	offline	slave /no heartbeat
18	mgt -b	online	master
19	power	online	warning
20	power	offline	
21	power	offline	
22	fan	offline	fail

Switch#

第 3 章 端口命令

3.1 端口通用配置

3.1.1 interface

命令

interface <if-name>

模式

全局配置模式/接口配置模式

参数

if-name: 端口名。百兆端口以 fe 为前缀,千兆端口以 ge 为前缀,万兆端口以 xe 为前缀,后加模块号/端口号。例:第一槽的 24gt 的第一端口表示为 ge1/1;第三槽的 10g2x 的第二端口表示为 xe3/2。

描述

interface命令用来进入某一个端口的配置模式。

举例

#进入第二槽的 24gx 的端口 24:

Switch(config)#interface ge2/24

3.1.2 bandwidth

命令

bandwidth <bandwidth>

no bandwidth [<bandwidth>]

模式

接口配置模式。

参数

bandwidth: 端口带宽。范围< 1-100000000000 bits> , 单位 : k, m, g。

描述

bandwidth命令用来指定端口的带宽。

no bandwidth命令取消端口带宽设置。默认不指定端口带宽。

举例

#指定端口 ge1/1 带宽为 100M :
Switch(config-ge1/1)#bandwidth 100m

3.1.3 description**命令**

description <line>
no description

模式

接口配置模式。

参数

line: 端口描述字符串。

描述

description 命令设置端口描述，可对端口做说明。
no description 命令取消端口描述的配置。

举例

#设置端口ge1/1的描述为：bulid 1 floor 5
Switch(config-ge1/1)#description bulid 1 floor 5

3.1.4 duplex**命令**

duplex {auto | full | half}
no duplex

模式

接口配置模式。

参数

auto: 双工状态为自适应。
full : 双工状态为全双工。
half : 双工状态为半双工。

描述

duplex 设置端口的双工状态。

no duplex 取消端口的双工设置。

举例

#将端口ge1/1的双工状态配置为全双工：

Switch(config-ge1/1)#duplex full

3.1.5 flowcontrol

命令

flowcontrol {receive | send} {off | on}

模式

接口配置模式

参数

receive：接受流控帧的能力。

send：发送流控帧的能力。

off：关闭功能。

on：打开功能。

描述

flowcontrol 命令用来打开或关闭端口的流控功能，可控制是否发送流控帧或是否处理接收到的流控帧。

举例

无。

3.1.6 show flowcontrol

命令

show flowcontrol [interface <if-name>]

模式

普通模式/特权模式

参数

if-name：接口名。

描述

查看端口流控的配置情况。

举例

无。

3.1.7 show interface

命令

show interface [<if-name> | switchport]

模式

普通模式/特权模式

参数

if-name : 接口名。

switchport: 显示二层接口的模式。

描述

show interface 命令不加参数显示所有的二层和三层接口的信息。指定接口名显示指定的二层或三层接口的信息。show interface switchport 显示所有二层接口的 vlan 模式信息。

举例

#显示 vlan1 接口的信息：

Switch>show interface vlan1

Interface vlan1

Hardware is VLAN, address is 0000.0000.0001

index 3 metric 1 mtu 1500 duplex -half arp ageing timeout 25

<UP,BROADCAST,RUNNING,MULTICAST>

VRF Binding: Not bound

inet 172.16.0.253/24 broadcast 172.16.0.255

input packets 0000039D0, bytes 0001E67CE, dropped 000000000,

multicast packe

ts 0000006DA

output packets 00000057C, bytes 00002E0B4, multicast packets

00000008A broad

cast packets 000003282

Switch>

Switch#show interface ge8/3

Interface ge8/3

Hardware is Ethernet, address is 0000.0000.0209


```
index 2451 metric 1 mtu 1500 duplex-half arp ageing timeout 0
<UP,BROADCAST,MULTICAST>
VRF Binding: Not bound
input packets 000000000, bytes 000000000, dropped 000000000,
multicast packets 000000000
output packets 000000000, bytes 000000000, multicast packets
000000000 broadcast packets 000000000
Switch#
```

3.1.8 shutdown

命令

```
shutdown
no shutdown
```

模式

接口配置模式

参数

无

描述

shutdown 关闭端口，端口的管理状态为 DOWN。
no shutdown 打开端口，端口的管理状态为 UP。

举例

```
#关闭端口 ge1/1:
Switch(config-ge1/1)#shutdown
Switch(config-ge1/1)#
```

3.2 MIRROR 命令

3.2.1 mirror

命令

```
mirror interface <if-name> direction {both | receive | transmit}
no mirror interface <if-name> direction [receive | transmit]
```

模式

接口配置模式。

参数

if-name: 被侦听端口。

both : 侦听指定端口的进出数据流。

receive : 侦听指定端口收到的数据流。

transmit : 侦听指定端口输出的数据流。

描述

mirror interface命令指定被侦听的端口，用来侦听其它端口的数据流。

no mirror interface 命令取消端口的侦听设置。

举例

#用端口ge1/1侦听端口ge1/12的输入数据流：

```
Switch(config-ge1/1)#mirror interface ge1/12 direction receive
```

```
Switch(config-ge1/1)#
```

3.2.2 show mirror

命令

```
show mirror [interface <if-name>]
```

模式

特权模式

参数

interface <if-name> : 端口名。

描述

show mirror 命令用来显示指定端口的 mirror 配置情况。

举例

无。

3.3 端口限速命令

3.3.1 portrate

命令

```
portrate egress <rate>
```

```
portrate ingress <rate>
```

模式

接口配置模式。

参数

egress：端口输出速率。

ingress：端口输入速率。

rate：设定的速率值，范围：1-1048512 kbits。

描述

设置端口最大的输入输出速率。最小限制值为 64Kbps，粒度也是 64 Kbps。

举例

#设置端口 ge1/2 输入限速 128Kbps：

```
Switch(config-ge1/2)#portrate ingress 128
```

```
Switch(config-ge1/2)#
```

3.3.2 show portrate

命令

```
show portrate [interface <if-name>]
```

模式

特权模式

参数

if-name：端口名。

描述

show portrate 命令用来显示指定端口的限速配置。

举例

无。

3.4 广播风暴控制命令

3.4.1 storm-control

命令

```
storm-control {broadcast | dlf | multicast} level <level>
```

```
no storm-control {broadcast | dlf | multicast} level <level>
```

模式

接口配置模式

参数

broadcast：控制广播包。

dif：控制目的未知的单播包。

multicast：控制组播包。

level：控制的百分比，100%为 2097151 packets/s。精确到小数点后一位。

实际控制值为 $2097151 * level / 100$ 。

描述

storm-control 命令用来设置端口对广播包、dif 包、组播包的转发限制。设置了 storm-control 的端口收到符合设置的数据流时会限制转发速度。

no storm-control 命令用来取消设置。

举例

#限制端口 ge1/1 对广播流的转发速度为 20971 packets/s:

Switch(config-ge1/1)#storm-control broadcast level 1

3.4.2 show storm-control

命令

show storm-control [<if-name>]

模式

特权模式

参数

if-name：端口名。

描述

show storm-control 命令用来显示 storm-control 的设置情况，显示内容包括广播包、dif 包、组播包的控制值和丢弃的包数量。

举例

#显示端口 ge1/1 的 storm-control 配置：

Switch#show storm-control ge1/1

Port	BcastLevel	BcastDiscards	McastLevel	McastDiscards	DifLevel	DifDiscards
ge1/1	100.00%		0	100.00%		0
	100.00%	0				

Switch#

第 4 章 vlan 命令

4.1 vlan 创建命令

4.1.1 vlan database

命令

vlan database

模式

全局配置模式

参数

无。

描述

进入 vlan 配置模式。

举例

#进入 vlan 配置模式：

Switch(config)#vlan database

Switch(config-vlan)#

4.1.2 vlan

命令

vlan <vlan-id>

no vlan <vlan-id>

模式

vlan 配置模式

参数

vlan-id：要创建的 vlan 号。取值范围：2 ~ 4094

描述

vlan 命令用来创建VLAN。需要注意的是VLAN 1 为缺省VLAN无法删除。

no vlan命令用来删除一个vlan。

举例

创建 vlan 2：

```
Switch(config-vlan)#vlan 2
Switch(config-vlan)#
```

4.2 vlan 端口配置命令

4.2.1 switchport access

命令

```
switchport access vlan <vlan-id>
no switchport access vlan
```

模式

接口配置模式

参数

vlan-id：端口的默认 VID，范围 2-4094。
缺省交换机中只有 VLAN 1，所有端口都是 VLAN1 的 untagged 成员。

描述

switchport access 命令用来设置 VLAN 模式是 ACCESS 的二层接口为指定的 VLAN。该命令只对 VLAN 模式是 ACCESS 模式的二层接口有效。设置此命令后，此二层接口的 PVID 是指定的 VLAN，此二层接口只属于指定的 VLAN 的 UNTAG 成员。

no switchport access vlan 命令把该接口的 access vlan 回复到缺省 VLAN，即 VLAN1。此命令设置后，此接口的 pvid 改为 1，并且只属于 VLAN1 的 untagged 成员。

举例

```
#将端口 ge1/1 配置为 vlan2 的 untagged 端口：
Switch(config-ge1/1)#switchport access vlan 2
```

4.2.2 switchport hybrid allowed vlan add

命令

```
switchport hybrid allowed vlan add <vlan-list> egress-tagged { disable |
enable}
```

模式

接口配置模式

参数

vlan-list : 加入 vlan 的 vlan 号, 范围 1-4094。

描述

switchport hybrid 命令用来把端口加入到指定的一个或多个 VLAN 中, 如果是 egress-tagged enable, 则是 TAG 成员, 如果是 egress-tagged disable, 则是 UNTAG 成员。

<vlan_list>有两种表达方式, 一种是以逗号分开的多个 VLAN 号 如 1,3,5,10, 另一种是一个 VLAN 范围, 如 2-10, 但两种方式不能同时存在。

表达方式 1,3-5 是错误的 (, 和 -只能存在一种), 2-4, 6-7 也是错误的 (-只能存在一次)。

举例

#将端口 ge1/1 设置为 vlan1-3 的 tagged 端口 :

```
Switch(config-ge1/1)#switchport mode hybrid
```

```
Switch(config-ge1/1)#switchport hybrid allowed vlan add 1-3  
egress-tagged enable
```

```
Switch(config-ge1/1)#
```

4.2.3 switchport hybrid allowed vlan all

命令

```
switchport hybrid allowed vlan all
```

模式

接口配置模式

参数

无

描述

switchport hybrid allowed vlan all 命令只对 hybrid 模式的二层接口有效。该接口加入到所有的 VLAN 中 (VLAN1 除外), 是所有的 VLAN 的 tagged 成员。以后新创建 VLAN 时, 该端口也会加入到新 VLAN 中, 是该 VLAN 的 TAG 成员。执行此命令后, 原来该端口是属于激活 vlan 的 UNTAG 成员会变为 TAG 成员。

举例

#将端口 ge1/1 设置为 vlan1 的 untagged 成员, 所有其它 vlan 的 tagged 成

员:

```
Switch(config-ge1/1)#switchport mode hybrid
```

```
Switch(config-ge1/1)#switchport hybrid allowed vlan all
```

4.2.4 switchport hybrid allowed vlan none

命令

```
switchport hybrid allowed vlan none
```

模式

接口配置模式

参数

无

描述

此命令只对 hybrid 模式的二层接口有效。该接口不再是所有的 VLAN 的成员（VLAN1 除外）。执行此命令后，该端口的 native vlan 会恢复为 1。

举例

#端口 ge1/1 原是 vlan1 的 tagged 端口 ,vlan2、vlan3 的 untagged 端口 ,vid=2 ;
将 ge1/1 从 vlan1 外的 vlan 删除:

```
Switch(config-ge1/1)#switchport hybrid allowed vlan none
```

执行该命令后，端口 ge1/1 是 vlan1 的 tagged 端口，vid=1。

4.2.5 switchport hybrid allowed vlan remove

命令

```
switchport hybrid allowed vlan remove <vlan-id>
```

模式

接口配置模式

参数

vlan-id : 需移除的 vlan 号，范围 1-4094。

描述

此命令只对 hybrid 模式的二层接口有效。该接口不再是指定的一个或多个 VLAN 的成员。

如果指定的 VLAN 中有激活的 vlan，则 native vlan 恢复到 1。

举例

#将端口 ge1/1 从 vlan2 中删除：

```
Switch(config-ge1/1)#switchport hybrid allowed vlan remove 2
```

4.2.6 switchport hybrid vlan

命令

```
switchport hybrid vlan <vlan-id>  
no switchport hybrid vlan
```

模式

接口配置模式

参数

vlan-id：加入的 vlan 的 vlan 号。

描述

此命令只对 hybrid 模式的二层接口有效。对于 hybrid 接口来说，把该接口的 native vlan 设置为指定的 VLAN。设置此命令后，此二层接口的 pvid 为指定的 VLAN，且该接口属于指定的 VLAN 的 untagged 成员（如果在设置此命令前，该端口已经属于该 VLAN 的 TAG 成员，则执行此命令后该端口继续保持为 TAG 成员，PVID 还是为指定的 VLAN）。

no switchport hybrid vlan 命令把该接口的 native vlan 恢复为缺省 VLAN（VLAN1）。执行此命令后，原来的 native vlan 删除（不再属于原来的 native vlan 的 UNTAG 或 TAG 成员），新的 native vlan 为 1，属于 VLAN1 的 UNTAG 成员（如果在执行此命令前，该端口已经是 VLAN1 的 TAG 成员，则执行此命令后继续保持为 VLAN1 的 TAG 成员），PVID 修改为 1。

举例

#配置端口 ge1/1 为 vlan2 的 untagged 成员，vlan1 的 tagged 成员，且 vid 为 2：

```
Switch(config-ge1/1)#switchport mode hybrid
```

```
Switch(config-ge1/1)#swi hybrid vlan 2
```

```
Switch(config-ge1/1)#switchport hybrid allowed vlan add 1 egress-tagged  
enable
```

4.2.7 switchport mode

命令

```
switchport mode { access | hybrid | trunk}
no switchport { access | hybrid | trunk}
```

模式

接口配置模式

参数

access : 接口 vlan 模式为 access 模式。缺省为 access 模式。如果二层接口设置为 ACCESS 模式 ,该接口缺省为 VLAN1 的 UNTAG 成员 ,PVID 为 1。

hybrid : 接口 vlan 模式为 hybrid 模式。如果接口设置为 HYBRID 模式 ,该接口缺省为 VLAN1 的 UNTAG 成员 ,PVID 为 1。

trunk : 接口 vlan 模式为 trunk 模式。如果接口设置为 TRUNK 模式 ,该接口缺省为 VLAN1 的 TAG 成员 ,PVID 为 1。

描述

设置二层接口的 VLAN 模式 ,是 access、 hybrid 或 trunk 中的一种。

no switchport 命令将接口模式恢复为缺省值 ,回到 access 模式 ,并且 access vlan 是 VLAN1。

举例

#设置端口 ge1/1 为 trunk 端口 :

```
Switch(config-ge1/1)#switchport mode trunk
```

4.2.8 switchport trunk allowed vlan add

命令

```
switchport trunk allowed vlan add <vlan-list>
```

模式

接口配置模式

参数

vlan-id : 该接口加入的一个或多个 VLAN 号。VLAN ID 的范围是 1-4094。
<vlan-id> 有两种表达方式 ,一种是以逗号分开的多个 VLAN 号 ,如 1,3,5,10 ,
另一种是一个 VLAN 范围 ,如 2-10 ,但两种方式不能同时存在。

描述

此命令只对 trunk 模式的二层接口有效。该接口加入到指定的一个或多个 VLAN 中 ,成为指定的 VLAN 的 tagged 成员。

举例

#端口 ge1/1 配置为 vlan1-10 的 tagged 成员：

```
Switch(config-ge1/1)#switchport trunk allowed vlan add 1-10
```

4.2.9 switchport trunk allowed vlan all

命令

```
switchport trunk allowed vlan all
```

模式

接口配置模式

参数

无

描述

此命令只对 trunk 模式的二层接口有效。该接口加入到所有的 VLAN 中（VLAN1 除外），是所有 VLAN 的 tagged 成员。以后新创建 VLAN 时，该端口也会加入到新 VLAN 中，是该 VLAN 的 TAG 成员。

举例

#端口 ge1/1 配置为所有 vlan 的 tagged 成员：

```
Switch(config-ge1/1)#switchport trunk allowed vlan all
```

4.2.10 switchport trunk allowed vlan none

命令

```
switchport trunk allowed vlan none
```

模式

接口配置模式

参数

无

描述

此命令只对 trunk 模式的二层接口有效。该接口不再是任何 VLAN 的成员（VLAN1 除外）。

举例

#将 trunk 端口 ge1/1 从 vlan1 外的其它 vlan 中删除：

```
Switch(config-ge1/1)#switchport trunk allowed vlan none
```

4.2.11 switchport trunk allowed vlan remove

命令

switchport trunk allowed vlan remove <vlan-list>

模式

接口配置模式

参数

vlan-list：将该接口删除的一个或多个 VLAN 号。VLAN ID 的范围是 1-4094。
vlan-list 有两种表达方式，一种是以逗号分开的多个 VLAN 号，如 1,3,5,10，
另一种是一个 VLAN 范围，如 2-10，但两种方式不能同时存在。

描述

此命令只对 trunk 模式的二层接口有效。该接口不再是指定的一个或多个 VLAN 的成员。

举例

#将端口 ge1/1 从 vlan 2 vlan3 中删除：
Switch(config-ge1/1)#switchport trunk allowed vlan remove 2,3

4.3 vlan 查看命令

4.3.1 show vlan

命令

show vlan [<vlan-id>]

模式

普通模式/特权模式

参数

vlan-id：需显示的 vlan 号，范围 1 - 4094。

描述

显示 VLAN 的信息，包括 VLAN 中的端口的信息。指定 vlan id 时只显示指定 vlan 的信息。

举例

#Switch>show vlan

VLAN	Name	State	Member ports ([u]-Untagged, [t]-Tagged)
1	vlan1	active	[u]ge1/1 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10 [u]ge1/11 [u]ge1/12[u]ge1/13 [u]ge1/14 [u]ge1/15 [u]ge1/16 [u]ge1/17[u]ge1/18 [u]ge1/19 [u]ge1/20 [u]ge1/21 [u]ge1/22 [u]ge1/23 [u]ge1/24
2	vlan2	active	[t]ge1/1
3	vlan3	active	[u]ge1/2

4.3.2 show interface switchport

命令	show interface switchport
模式	普通模式/特权模式。
参数	无。
描述	显示端口的 VLAN 模式和 PVID 等信息。
举例	无。

第 5 章 MSTP 命令

5.1 MSTP 配置命令

5.1.1 spanning-tree mst cisco-interoperability

命令

spanning-tree mst ciscointeroperability {disable | enable}

模式

全局配置模式

参数

disable：关闭功能。默认关闭。

enable：打开功能。

描述

启动或关闭和 cisco 的生成树协议的兼容。

联想天工网络交换机采用基于 802.1s 的 MSTP 协议，每个 MSTI 消息的长度是 16 个字节；而 CISCO 交换机的 BPDU 每个 MSTI 消息的长度是 26 个字节。为了和 CISCO 交换机互用，配置联想天工网络的交换机时要启动和 CISCO 兼容的开关。

举例

无。

5.1.2 spanning-tree mst configuration

命令

spanning-tree mst configuration

模式

全局配置模式

参数

无

描述

进入 spanning-tree 的配置模式。

举例

无。

5.1.3 spanning-tree mst enable

命令

spanning-tree mst enable

模式

全局配置模式

参数

无

描述

启动 mstp 计算。

举例

无。

5.1.4 spanning-tree mst errdisable-timeout

命令

spanning-tree mst errdisable-timeout {enable | interval <seconds>}
no spanning-tree mst errdisable-timeout {enable | interval}

模式

全局配置模式

参数

seconds：超时时间，范围 10-1000000 秒。默认 300 秒。

描述

spanning-tree mst errdisable-timeout enable 命令启动 errdisable 机制，当启动 BPDU guard 的端口收到 BPDU 时，会启动 errdisable timer。errdisable 会在系统配置的超时时间后重新启动这个端口。

spanning-tree mst errdisable-timeout interval 命令设置 errdisable 超时时间。

no spanning-tree mst errdisable-timeout 命令用来取消相应配置，恢复默认值。

举例

无。

5.1.5 spanning-tree mst forward-time

命令

spanning-tree mst forward-time <seconds>
no spanning-tree mst forward-time

模式

全局配置模式。

参数

seconds：端口从 discarding 到 learning 以及 learning 到 forwarding 等待的秒数。范围 4-30 秒。默认 15 秒。

根据生成树协议 forward-time 必须满足下列条件：

$2 * (\text{forward-time} - 1) \geq \text{max-age}$ 。

描述

spanning-tree mst forward-time 命令用来配置转发延迟时间。

no spanning-tree mst forward-time 命令用来取消转发延时配置，恢复默认值。

举例

无。

5.1.6 spanning-tree mst hello-time

命令

spanning-tree mst hello-time <seconds>
no spanning-tree mst hello-time

模式

全局配置模式

参数

seconds：根交换机产生配置信息的间隔时间。范围 1-10 秒。默认 2 秒。

根据生成树协议 hello-time 必须满足下列条件：

$2 * (\text{hello-time} + 1) \leq \text{max-age}$ 。

描述

spanning-tree mst hello-time 配置 MSTP hello 报文发送间隔时间。

no spanning-tree mst hello-time 命令取消配置，恢复默认值。

举例

#配置 hello 报文发送间隔为 10 秒：

Switch(config)#spanning-tree mst hello-time 10

5.1.7 spanning-tree mst max-age

命令

spanning-tree mst max -age <seconds>

no spanning-tree mst max-age

模式

全局配置模式

参数

seconds：交换机在触发一个重新配置前，等待接收生成树配置信息的秒数。

范围 6-40 秒。默认 20 秒。

描述

配置侦听根桥的最大时间。

no 命令取消配置，恢复默认值。

举例

无。

5.1.8 spanning-tree mst max-hops

命令

spanning-tree mst max -hops <hops>

no spanning-tree mst max-hops

模式

全局配置模式

参数

hops：在一个域中在 BPDU 被丢弃前指定的跳数。范围 1-40。默认 20 跳。

描述

配置 BPDU 协议包有效的最大跳数。

no 命令取消配置，恢复默认值。

举例

无。

5.1.9 spanning-tree mst portfast

命令

spanning-tree mst portfast
no spanning-tree mst portfast

模式

接口配置模式

参数

无

描述

spanning-tree mst portfast 命令配置一个端口为 portfast 端口，可使端口从 blocking 状态到 forwarding 状态，绕过 listening 和 learning 状态。
no 命令取消配置，恢复默认值。

举例

#配置端口 ge1/1 为 portfast 接口：
Switch(config-ge1/1)#spanning-tree mst portfast

5.1.10 spanning-tree mst portfast bpdu-filter

命令

spanning-tree mst portfast bpdu-filter [default | disable | enable]
no spanning-tree mst portfast bpdu-filter

模式

全局配置模式和接口配置模式

参数

default：默认状态。
disable：关闭功能。
enable：启用功能。

描述

防止 portfast 端口接收或发送 BPDU。
在全局配置模式，spanning-tree mst portfast bpdu-filter 命令启动在 portfast bpdu-filter default 状态的端口的 BPDU filtering 功能。在接口配置模式，

spanning-tree mst portfast bpdu-filter enable 在任意端口打开 BPDU filter。
no 命令取消配置，恢复默认值。

举例

#配置端口 ge1/1 为 portfast 接口，且不发送 mstp bpdu 包：

```
Switch(config-ge1/1)#spanning-tree mst portfast
```

```
Switch(config-ge1/1)#spanning-tree mst portfast bpdu-filte enable
```

5.1.11 spanning-tree mst portfast bpdu-guard

命令

```
spanning-tree mst portfast bpdu-guard [default | disable | enable]
```

```
no spanning-tree mst portfast bpdu-guard
```

模式

全局配置模式和接口配置模式

参数

default：默认状态。

disable：关闭功能。

enable：启用功能。

描述

当配置了 BPDU gurad 的端口收到 BPDU 时，spanning tree 会 shutdown 这个的端口。在一个有效的配置，Port Fast-enabled 的端口不接收 BPDU。在一个 portfast enabled 的端口接收到一个 BPDU 表示一个无效的配置，例如是一个未经授权设备的连接，BPDU guard 进入到一个 error-disabled 状态。

no 命令取消配置，恢复默认值。

举例

#配置端口 ge1/1 为 portfast 接口，启用 BPDU 保护功能：

```
Switch(config-ge1/1)#spanning-tree mst portfast
```

```
Switch(config-ge1/1)#spanning-tree mst portfast bpdu-guard enable
```

5.1.12 spanning-tree mst priority

命令

```
spanning-tree mst priority <value>
```

模式

全局配置模式

参数

value : CIST bridge 的优先级，范围 0-61440，默认值为 32768。CIST 优先级的值只能是 4096 的倍数。

描述

配置桥优先级。桥优先级低的设备更有可能成为根桥。

举例

```
#配置 CIST 桥优先级为 36862 :  
Switch#configure terminal  
Switch(config)#spanning-tree mst priority 36862
```

5.1.13 instance

命令

```
instance <instance-id> [priority <value> | vlan <vlan-id>]  
no instance <instance-id> [vlan <vlan-id> ]
```

模式

MSTP 配置模式

参数

instance-id : 要创建的实例号，范围 1-15。
value : 优先级的值，范围 0-61440，粒度 4096。默认值为 32768。
vlan-id : 添加到实例的 vlan 号。

描述

instance <instance-id> 命令创建实例。
instance <instance-id> priority <value> 命令配置 MSTI bridge 的优先级。
instance <instance-id> vlan <vlan-id> 命令添加实例 vlan。
no instance <instance-id> 命令删除实例。
no instance <instance-id> vlan <vlan-id> 命令删除 vlan 与实例的关联。

举例

```
#创建 MSTP 实例 2，添加 vlan2、vlan3 :  
Switch(config-mst)#instance 2  
Switch(config-mst)#instance 2 vlan 2  
Switch(config-mst)#instance 2 vlan 3
```

5.1.14 region

命令

region <region-name>

no region

模式

MSTP 配置模式

参数

region-name : MSTP 域的域名, 长度 1 - 32 个字符。

no 命令取消域名配置。

描述

配置域名。

举例

无。

5.1.15 revision

命令

revision <revision-num>

模式

MSTP 配置模式

参数

revision-num : 修订版本号, 范围 0-255。

描述

配置修订版本号。

举例

无。

5.1.16 spanning-tree mst force-version

命令

spanning-tree mst force-version <version>

no spanning-tree mst force-version

模式

接口配置模式

参数

version：协议的类型，范围 0-3，0 代表 STP 协议，1 代表不支持生成树，2 代表 RSTP 协议，3 代表 MSTP 协议。默认协议类型为 0。

描述

配置发送协议包的类型。

no 命令取消配置，恢复默认值。

举例

#配置端口 ge1/1 发送 stp 协议包：

```
Switch(config-ge1/1)# spanning-tree mst force-version 0
```

5.1.17 spanning-tree mst guard root

命令

```
spanning-tree mst guard root
```

```
no spanning-tree mst guard root
```

模式

接口配置模式

参数

无

描述

配置启动 root guard 功能，不接收桥优先级比自己高的 BPDU 包，指定该交换机为根交换机。默认关闭。

no 命令取消配置，恢复默认值。

举例

无。

5.1.18 spanning-tree mst instance

命令

```
spanning-tree mst instance <instance-id> [path-cost <cost> | priority  
<value>]
```

```
no spanning-tree mst instance <instance-id> [path-cost <cost>]
```

模式

接口配置模式

参数

instance-id : 实例号。范围 1 - 15。

cost : 路径开销值，范围 1-200000000。较低的路径开销更可能成为根。默认值 20000000。

priority <value> : MSTI 优先级的值，范围 0-240，只能是 16 的倍数。优先级值较低的更可能成为根。

描述

spanning-tree mst instance <instance-id> 命令把接口加入实例。

spanning-tree mst instance <instance-id> path-cost <cost> 命令设置 msti 路径开销。

spanning-tree mst instance <instance-id> priority <value> 命令设置 msti 优先级。

no 命令取消配置，恢复默认值。

举例

#把端口 ge1/1 加入到实例 2，并配置端口的路径开销为 10，优先级为 160：

```
Switch(config-ge1/1)#spanning-tree mst ins 2 path-cost 10
```

```
Switch(config-ge1/1)#spanning-tree mst ins 2 priority 160
```

```
Switch#sh spanning-tree mst ins 2 inter ge1/1
```

```
% ge1/1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding
```

```
% ge1/1: Designated Internal Path Cost 0 - Designated Port Id 0
```

```
% ge1/1: Configured Internal Path Cost 10
```

```
% ge1/1: Configured CST External Path cost 20000000
```

```
% ge1/1: CST Priority 128 - MSTI Priority 160
```

```
% ge1/1: Designated Root 0000000000000207
```

```
% ge1/1: Designated Bridge 0000000000000207
```

```
% ge1/1: Message Age 0 - Max Age 0
```

```
% ge1/1: Hello Time 0 - Forward Delay 0
```

```
% ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

5.1.19 spanning-tree mst link-type

命令

```
spanning-tree mst link-type { point-to-point | shared}
```

```
no spanning-tree mst link -type
```

模式

接口配置模式

参数

point-to-point：连接类型为点到点，允许端口状态快速转换。为默认类型。
shared：连接类型为共享，不允许端口状态快速转换，要经过 802.1D 的计算过程来确定端口的状态。。

描述

配置接口的连接类型。
no 命令取消配置，恢复默认值。

举例

无。

5.1.20 spanning-tree mst path-cost

命令

spanning-tree mst path-cost <cost>
no spanning-tree mst path-cost

模式

接口配置模式

参数

cost：cist 路径开销值，范围 1-200000000。默认值 20000000。较低的路径开销更可能成为根。
下面是带宽和路径花消映射表：

带宽(bps)	路径花消
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>10000000000000	2

描述

配置 cist 路径开销。

no 命令取消配置，恢复默认值。

举例

#配置实例 2 中端口 ge1/1 的 cist 路径开销为 200：

```
Switch(config-ge1/1)#spanning-tree mst path-cost 200
```

```
Switch#show spanning-tree mst instance 2 interface ge1/1
```

```
% ge1/1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding
```

```
% ge1/1: Designated Internal Path Cost 0 - Designated Port Id 0
```

```
% ge1/1: Configured Internal Path Cost 20000000
```

```
% ge1/1: Configured CST External Path cost 200
```

```
% ge1/1: CST Priority 128 - MSTI Priority 128
```

```
% ge1/1: Designated Root 0000000000000207
```

```
% ge1/1: Designated Bridge 0000000000000207
```

```
% ge1/1: Message Age 0 - Max Age 0
```

```
% ge1/1: Hello Time 0 - Forward Delay 0
```

```
% ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

5.1.21 spanning-tree mst priority

命令

```
spanning-tree mst priority <value>
```

模式

接口配置模式

参数

value：cist 端口的优先级，范围 0-240，只能是 16 的倍数。默认值 128。

描述

配置接口的 cist 优先级。

举例

#配置实例 2 端口 ge1/1 的 cist 优先级为 240：

```
Switch(config-ge1/1)#spanning-tree mst priority 240
```

```
Switch#show spanning-tree mst instance 2 interface ge1/1
```

```
% ge1/1: Port 2001 - Id f7d1 - Role Disabled - State Forwarding
```

```
% ge1/1: Designated Internal Path Cost 0 - Designated Port Id 0
```

```
% ge1/1: Configured Internal Path Cost 10
```

```
% ge1/1: Configured CST External Path cost 20000000
```

```
% ge1/1: CST Priority 240 - MSTI Priority 160
```

```
% ge1/1: Designated Root 0000000000000207
% ge1/1: Designated Bridge 0000000000000207
% ge1/1: Message Age 0 - Max Age 0
% ge1/1: Hello Time 0 - Forward Delay 0
% ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

5.1.22 clear spanning-tree detected protocols

命令

```
clear spanning-tree detected protocols [interface <if-name>]
```

模式

特权模式

参数

if-name：需要复位 STP 协议侦察功能的端口。

描述

为了和 802.1D STP 协议的兼容，系统可以自动侦察对方系统运行的协议，根据对方运行的协议来决定这个端口运行的协议。clear spanning-tree detected protocols 命令复位这个协议协商的任务让它重新协商它和主机之间的协议。

举例

```
#关闭模块 1端口1的STP协议侦察功能：
clear spanning-tree detected protocols interface ge1/1
```

5.2 MSTP 查看命令

5.2.1 show spanning-tree mst

命令

```
show spanning-tree mst [config | detail | instance <instance-id> [interface
<if-name>] | interface <if-name>]
```

模式

普通模式/特权模式

参数

instance-id：实例号，范围 0 - 15。

if-name : 接口号。

描述

show spanning-tree mst 命令显示 cist 信息以及 vlan 和 instance 的对应表。

show spanning-tree mst config 命令显示 mstp 的配置信息。

show spanning-tree mst detail 命令显示 mstp 的详细信息 ,包括 cist 接口信息 ,实例信息和实例接口信息。

show spanning-tree mst instance <instance-id> 命令显示一个实例的信息。

show spanning-tree mst instance <instance-id> interface <if-name> 命令显示一个 cist 接口的信息。

show spanning-tree mst interface <if-name> : 显示一个 msti 接口的信息。

举例

#显示 mstp 配置信息 :

```
Switch#show spanning-tree mst config
```

```
%
```

```
% MSTP Configuration Information for bridge 1 :
```

```
%-----
```

```
% Format Id      : 0
```

```
% Name           : lenovo 12800
```

```
% Revision Level : 1
```

```
% Digest         : 0xD042DCDBBC60C63B623C157F60A37A6F
```

```
%-----
```

#显示实例 1 内接口 ge1/1 的 mstp 信息 :

```
Switch#show spanning-tree mst instance 1 interface ge1/1
```

```
% ge1/1: Port 2001 -Id 87d1 - Role Disabled - State Discarding
```

```
% ge1/1: Designated Internal Path Cost 0 - Designated Port Id 0
```

```
% ge1/1: Configured Internal Path Cost 20000000
```

```
% ge1/1: Configured CST External Path cost 20000
```

```
% ge1/1: CST Priority 128 - MSTI Priority 128
```

```
% ge1/1: Designated Root 0000000000000000
```

```
% ge1/1: Designated Bridge 0000000000000000
```

```
% ge1/1: Message Age 0 - Max Age 0
```

```
% ge1/1: Hello Time 0 - Forward Delay 0
```

```
% ge1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

5.3 MSTP 调试命令

5.3.1 debug mstp

命令

debug mstp
no debug mstp

模式

特权模式。

参数

无。

描述

debug mstp 命令用来打开 mstp 协议相关的调试开关，将相关日志写入日志表中。

no debug mstp 命令关闭 mstp 的调试开关。

举例

```
#打开 mstp 调试开关
Switch#debug mstp
Switch#
```

5.3.2 debug mstp all

命令

debug mstp all
no debug mstp all

模式

特权模式。

参数

无。

描述

debug mstp all 命令用来打开所有 mstp 协议相关的调试开关，将相关日志写入日志表中。

no debug mstp all 命令关闭 mstp 的调试开关。

举例

```
#打开 mstp 协议所有调试开关：
```

```
Switch#debug mstp all
Switch#
```

5.3.3 debug mstp cli

命令

```
debug mstp cli
no debug mstp cli
```

模式

特权模式。

参数

无。

描述

debug mstp cli 命令用来打开 mstp 协议相关的命令调试开关，将相关日志写入日志表中。

no debug mstp cli 命令关闭 mstp 的命令调试开关。

举例

#打开 mstp 协议命令调试开关：

```
Switch#debug mstp cli
Switch#
```

5.3.4 debug mstp packet

命令

```
debug mstp packet [recv | send]
no debug mstp packet [recv | send]
```

模式

特权模式。

参数

无。

描述

debug mstp packet 命令用来打开 mstp 协议报文调试开关，将相关日志写入日志表中。

no debug mstp packet 命令用来关闭 mstp 的报文调试开关。

举例

```
#打开 mstp 协议报文接收调试开关 :  
Switch#debug mstp packet recv  
Switch#
```

5.3.5 debug mstp protocol**命令**

```
debug mstp protocol [detail]  
no debug mstp protocol [detail]
```

模式

特权模式。

参数

无。

描述

debug mstp protocol 命令用来打开 mstp 协议报文调试开关，将相关日志写入日志表中。

no debug mstp protocol 命令用来关闭 mstp 的报文调试开关。

举例

```
#打开 mstp 协议详细调试开关 :  
Switch#debug mstp protocol detail  
Switch#
```

5.3.6 debug mstp timer**命令**

```
debug mstp timer [detail]  
no debug mstp timer [detail]
```

模式

特权模式。

参数

无。

描述

debug mstp timer 命令用来打开 mstp 协议的定时器调试开关，将相关日志写

入日志表中。

no debug mstp timer 命令用来关闭 mstp 的定时器调试开关。

举例

#打开 mstp 协议定时器调试开关：

```
Switch#debug mstp timer detail
```

```
Switch#
```

第 6 章 IGMP SNOOPING 命令

6.1 IGMP SNOOPING 配置命令

6.1.1 ip igmp snooping

命令

ip igmp snooping
no ip igmp snooping

模式

全局配置模式

参数

无

描述

ip igmp snooping 命令用来启动所有 vlan 的 igmp snooping 功能。
no ip igmp snooping 命令关闭所有 vlan 的 igmp snooping 功能。

举例

无。

6.1.2 ip igmp snooping fast-leave

命令

ip igmp snooping fast-leave vlan <vlan-id>
no ip igmp snooping fast-leave vlan <vlan-id>

模式

全局配置模式

参数

vlan-id：启动立即离开的 vlan 号。

描述

启动一个 vlan 的 IGMP V2 立即离开功能。
no 命令关闭一个 vlan 的 IGMP V2 立即离开功能。

举例

#启动 vlan2 的组播成员立即离开功能：

Switch(config)#ip igmp snooping fast-leave vlan 2

6.1.3 ip igmp snooping fast-leave-timeout

命令

ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>
no ip igmp snooping fast-leave-timeout vlan <vlan-id>

模式

全局配置模式

参数

interval：延时时间，单位 ms，范围无限制。默认为 300000 ms。

vlan-id：所配置的 vlan 的 vlan 号，范围 1 - 4094。

描述

设置一个 vlan 的组播成员立即离开延时时间，收到 leave 包后等待 interval 指定的时间才将成员删除。

no 命令取消立即离开延时设置，interval 恢复默认值。

举例

#配置 vlan1 收到组播成员的 leave 包后立即删除该成员：

Switch(config)#ip igmp snooping fast-leave vlan 1

Switch(config)#ip igmp snooping fast-leave-timeout 0 vlan 1

6.1.4 ip igmp snooping group-membership-timeout

命令

ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>
no ip igmp snooping group-membership-timeout vlan <vlan-id>

模式

全局配置模式

参数

interval：成员生存时间，单位 ms，范围无限制。默认 400000 ms。

vlan-id：所配置的 vlan 的 vlan 号，范围 1 - 4094。

描述

配置收到 report 包后加入的组播组的生存时间。

no 命令取消成员生存时间的配置，恢复默认值。

举例

#配置 vlan2 的组播成员生存时间为 600 秒：

```
Switch(config)#ip igmp snooping group-membership-timeout 600000 vlan  
2
```

6.1.5 ip igmp snooping mrouter

命令

```
ip igmp snooping mrouter interface <if-name> [vlan <vlan-id>]  
no ip igmp snooping mrouter interface <if-name> [vlan <vlan-id>]
```

模式

全局配置模式

参数

if-name：接口名。

vlan-id：接口所属 vlan 号。

描述

配置查询端口，其它端口收到收到组播加入离开包都会转发到该端口；该端口会加入组播组。

no 命令删除配置的查询端口。

举例

#配置端口 ge1/1 为 vlan2 的查询端口：

```
Switch(config)#ip igmp snooping mrouter interface ge1/1 vlan 2
```

6.1.6 ip igmp snooping query-membership-timeout

命令

```
ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>  
no ip igmp snooping query-membership-timeout vlan <vlan-id>
```

模式

全局配置模式

参数

interval 查询端口的生存时间,单位 ms,范围 60000-300000ms。默认 300000 ms。

vlan-id：所配置的 vlan 的 vlan 号，范围 1 - 4094。

描述

配置收到 QUERY 包后加入的查询组的生存时间。

no 命令取消查询组生存时间的配置，恢复默认值。

举例

#配置 vlan2 的查询端口时间为 600 秒：

```
Switch(config)#ip igmp snooping query-membership-timeout 600000 vlan 2
```

6.1.7 ip igmp snooping vlan

命令

```
ip igmp snooping vlan <vlan-id>
```

```
no ip igmp snooping vlan <vlan-id>
```

模式

全局配置模式

参数

vlan-id：vlan 号。

描述

启动一个 vlan 的 igmp snooping 功能，必须先执行 ip igmp snooping 后才能

配置一个 vlan 的 igmpsnoop 功能。

no 命令关闭一个 vlan 的 igmp snooping 功能。

举例

#关闭 vlan3 的 igmp snooping 功能，其它 vlan 打开 igmp snooping 功能：

```
Switch(config)#no ip igmp snooping vl
```

```
Switch(config)#no ip igmp snooping vlan 3
```

6.2 IGMP SNOOPING 查看命令

6.2.1 show ip igmp snooping

命令

```
show ip igmp snooping [fast-leave [vlan <vlan-id>] | fast-leave-timeout  
[vlan <vlan-id>] | forwarding-table | group-membership-timeout [vlan  
<vlan-id>] | interface [vlan <vlan-id>] | query-membership-timeout [vlan
```

<vlan-id>] | vlan <vlan-id>]

模式

普通模式/特权模式

参数

fast-leave：显示立即离开功能的打开情况。

vlan <vlan-id>：显示指定 vlan 的配置。

fast-leave-timeout：显示立即离开延时时间的配置。

forwarding-table：显示组播转发表，包括组播组和对应的 vlan、端口。

group-membership-timeout：显示组成员生存时间配置。

interface：显示可使用的端口和 vlan 的关系。

query-membership-timeout：显示查询组生存时间配置。

vlan：显示指定 vlan 的 igmp snooping 配置。

描述

显示 igmp snooping 配置。

举例

#显示 vlan1 的 igmp snooping 配置：

```
Switch#show ip igmp snooping vlan 1
```

```
Bridge 1 VLAN 0:
```

```
IGMP Snooping is globally enabled
```

```
Bridge 1: VLAN 1
```

```
    IGMP Snooping is enabled
```

```
    IGMP Snooping fast-leave is enabled
```

```
    IGMP Snooping fast-leave-timeout is 300000 ms
```

```
    IGMP snooping query membership timeout is 300000 ms
```

```
    IGMP snooping group membership timeout is 400000 ms
```

6.2.2 show ip igmp snooping age-table

命令

```
show ip igmp snooping age-table { group-membership |
query-membership}
```

模式

普通模式/特权模式

参数

group-membership : 显示成员组的 age 时间。

query-membership : 显示查询组的 age 时间。

描述

显示组播组的 age 时间、所在端口的情况。

举例

#显示成员组的 age 时间 :

Switch#show ip igmp snooping age-table group-membership

VLAN	Address	Port	Seconds
3	239.255.255.250	ge1/2	340000 ms

6.2.3 show ip igmp snooping mrouter

命令

show ip igmp snooping mrouter [interface <if-name> | vlan <vlan-id>]

模式

普通模式/特权模式

参数

interface <if-name> : 显示指定端口能

vlan <vlan-id> : 显示指定 vlan 的查询端口。

描述

显示查询端口信息。

举例

#显示 vlan3 的查询端口 :

Switch#show ip igmp snooping mrouter vlan 3

Bridge	VLAN	Ports
-----	-----	-----
	1	3 ge1/2,

6.2.4 show ip igmpv2

命令

show ip igmpv2 snooping statistics [vlan <vlan-id>]

模式

普通模式/特权模式

参数

vlan <vlan-id> : 显示指定的 vlan 的情况。

描述

显示 igmpv2 协议包的统计数据。

举例

#显示 vlan1 的 igmpv2 协议包统计：

```
Switch#show ip igmpv2 snooping statistics vlan 1
```

```
IGMP-V2 Snooping Statistics: Bridge 1  VLAN default
```

```
Total valid pkts rcvd : 0
```

```
Total invalid pkts rcvd : 0
```

```
Number of Reports rcvd : 0
```

```
Number of Leaves rcvd : 0
```

```
Number of Membership Queries rcvd : 0
```

```
Number of Reports tx : 0
```

```
Number of Leaves tx : 0
```

```
Number of Group-Specific Queries tx : 0
```

```
Number of General Queries tx : 0
```

6.3 IGMP SNOOPING 调试命令

6.3.1 debug igmp snooping

命令

```
debug igmp snooping [all] | [cli] | [events] | [packet] | [timer]
```

```
no debug igmp snooping [all] | [cli] | [events] | [packet] | [timer]
```

模式

特权模式。

参数

all : 打开 igmp snooping 所有得调试开关。

cli : cli 命令提示。

events : 打开 igmp snooping 时间调试开关。

packet : 打开 igmp snooping 报文调试开关。

timer : 打开 igmp snooping 定时器调试开关。

描述

debug igmp snooping 命令用来打开 igmp snooping 相关调试开关，使用户能够看到 igmp snooping 的相关事件和报文收发情况。

no debug igmp snooping 命令关闭对应的 igmp snooping 调试开关。

举例

#打开 igmp snooping 报文调试开关：

```
Switch#debug igmp snooping packet
```

```
Switch#
```

第 7 章 ACL 命令

7.1 ACL 配置命令

7.1.1 基于标准 IP 的 ACL 规则

命令

access-list {<group-id>} {permit | deny | remark} {<source-ip>}

模式

全局配置模式

参数

group-id：规则组号，范围：<1-99>|<1300-1999>。

permit：允许符合规则的数据包转发。

deny：禁止符合规则的数据包转发。

remark：给指定规则组添加注释。

source-ip：源 IP，有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的 IP 地址；

2) any 相当于 A.B.C.D 255.255.255.255

3) host A.B.C.D 相当于 A.B.C.D 0.0.0.0

wildcard：决定哪些 bits 需要匹配，'0' 表示需要匹配，'1' 表示不需要匹配。

描述

配置基于标准 IP 的 ACL 访问控制规则。这一类规则只是判断数据包的源 IP 地址是否匹配已经配置了的 ACL 规则；如果匹配了根据 deny/permit 作相应的处理。在所有的 ACL 规则中都有一条 deny 所有 IP 包的隐藏规则，只要用户配置了一条 ACL 规则，系统会自动产生这条规则。因此用户不需要手动去 deny any 的配置。基于扩展 IP 规则和基于 MAC 地址规则也是如此。

举例

#配置一组规则，允许源地址为 192.168.0.0 网段的数据包转发，禁止源地址为 192.168.0.11 和其它地址的数据包转发：

```
Switch(config)#access-list 1 deny host 192.168.0.11
```

```
Switch(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

```
Switch(config)#access-list 1 deny any
```


7.1.2 基于扩展 IP 的 ACL 规则

命令

```
access-list {<group-id>} {permit | deny | remark} {protocol} {<source-ip>}  
[<source-port>] {<dest-ip>} [<type> | <dest-port>]
```

模式

全局配置模式

参数

group-id：规则组号，范围<100-199>|<2000-2699>。

permit：允许符合规则的数据包转发。

deny：禁止符合规则的数据包转发。

remark：给指定规则组添加注释。

protocol：在IP 层之上的协议类型，如：icmp，igmp，ospf，tcp，udp 等，也可以输入相应的数字，如6代表tcp。如果不需要对这些协议进行控制，可以输入ip 或(0)。

source-ip：源IP，有三种输入方式：

- 1) A.B.C.D wildcard 可以控制来自一个网段的IP地址；
- 2) any 相当于A.B.C.D 255.255.255.255
- 3) host A.B.C.D相当于A.B.C.D 0.0.0.0

wildcard：决定哪些 bits 需要匹配，'0'表示需要匹配，'1'表示不需要匹配。

source-port：是对于 protocol 为 tcp 或 udp 的情况，可以控制数据包的源端口，输入方式可以是一些熟悉的端口服务名称，如：www，也可以是数字，如 80 代表 www 端口。

dest-ip：目的IP地址。有三种输入方式：

- 1) A.B.C.D wildcard 可以控制来自一个网段的IP地址；
- 2) any 相当于A.B.C.D 255.255.255.255
- 3) host A.B.C.D相当于A.B.C.D 0.0.0.0

type：是对于 protocol 为 icmp 或 igmp 的情况，可以控制消息类型，输入方式可以是消息类型名称，如 echo、leave，也可以是数字，如 8 代表 icmp echo 包。

dest-port : 是针对 protocol 为 tcp 或 udp 的情况 , 可以控制数据包的目的端口 , 输入方式和 srcPort 相同。

描述

配置一条扩展 ip 规则 , 匹配指定协议包 , 可根据数据包的源和目的 IP 地址、消息类型或端口决定转发或丢弃。

举例

#配置规则禁止从 192.168.0.2 到 192.168.1.0 网段的 ip 包 , 允许 192.168.0.2 到 192.168.2.1 的 ospf 包 :

```
Switch(config)#access-list 100 deny ip host 192.168.0.2 192.168.1.0 0.0.0.255
```

```
Switch(config)#access-list 100 permit ospf host 192.168.0.2 host 192.168.2.1
```

#配置一组规则 , 要实现 10.1.0.0 255.255.0.0 网段的地址不能访问任何的 www 服务器 , 但是 10.1.1.1 不作上述的限制 ; 可以作如下配置 :

```
switch# access-list 200 deny tcp 10.1.0.0 0.0.255.255 any www
```

```
switch# access-list 200 permit tcp host 10.1.1.1 any www
```

7.1.3 字符类型的 ACL 规则

命令

```
access-list {<rule-name>} {permit | deny | remark}  
{ <source-ip> }[exact-match]
```

模式

全局配置模式

参数

rule-name : 规则名。

permit : 允许符合规则的数据包转发。

deny : 禁止符合规则的数据包转发。

remark : 给指定规则组添加注释。

source-ip : 源 IP , 有两种输入方式 :

1) A.B.C.D/M 需匹配的前缀 , 如 10.0.0.0/8

2) any 相当于 0.0.0.0/0

A.B.C.D/M 中 M 表示需要匹配的位数。

exact-match : 精确匹配。如果配置 exact-match 相当于 host。

描述

配置一组以字符串命名的规则，只供路由协议调用。

举例

#配置一组名字为 room1 的规则，允许 172.16.2.0 网段的地址，禁止 172.16.2.1 的地址：

```
Switch(config)#access-list room1 deny 172.16.2.1/32 exact-match
```

```
Switch(config)#access-list room1 permit 172.16.2.0/24
```

7.1.4 access-group

命令

```
access-group <group-id>
```

模式

接口配置模式

参数

group-id：引用的规则组号，标准 IP 规则范围<1-99>|<1300-1999>，扩展 IP 规则范围<100-199>|<2000-2699>。

描述

在端口引用一组 acl 规则。

举例

#在端口 ge1/1 引用规则组 1：

```
Switch(config-ge1/1)#access-group 1
```

7.2 ACL 查看命令

7.2.1 show access-group

命令

```
show access-group
```

模式

普通模式/特权模式

参数

无

描述

显示 acl 规则的引用情况。

举例

```
#Switch#show access-group
Interface ge1/1
access-list 100 is set
```

7.2.2 show access-list

命令

```
show access-list [<group-id>]
```

模式

特权模式

参数

group-id : 要显示的规则号。

描述

显示配置的 acl 规则。

举例

```
#Switch#show access-list
```

Standard IP access list 1, Remark acl1

```
deny 192.168.1.0, wildcard bits 0.0.0.255
permit any
```

Extended IP access list 100,

```
permit ospf host 192.168.0.2 host 192.168.2.1
permit ip host 192.168.0.2 192.168.1.0 0.0.0.255
```

第 8 章 IP 路由命令

8.1 配置命令

8.1.1 arp

命令

```
arp <ip-address> <mac-address>  
no arp {<ip-address> | <ip-prefix>}
```

模式

全局配置模式

参数

ip-address：IP 地址。
mac-address：mac 地址，格式 HHHH.HHHH.HHHH。
ip-prefix：ip 前缀，使用 ip 地址/掩码形式，表示一个网络。

描述

arp 命令用来配置静态 arp 表项。
no arp 命令用来删除对应的 arp 表项。

举例

```
#配置 ip 地址 192.168.1.1 与 MAC 地址 0003.0010.1011 映射  
Switch(config)#arp 192.168.1.1 0003.0010.1011  
Switch(config)#
```

8.1.2 arp lock

命令

```
arp lock <ip-prefix>  
arp unlock {<ip-prefix> | all}
```

模式

全局配置模式

参数

ip-prefix：IP 地址段，格式 A.B.C.D/M。
all:所有网络。

描述

arp lock 命令用来锁住一个网段，执行该命令后，对应网段内所有动态 arp 表项被删除且不再学习新的 arp 表项。仅保留静态 arp 表项，且不会过期。
arp unlock 命令用来对对应网段进行解锁定。

举例

#对 172.20.0.0/16 网段上锁，不再学习新的 arp
Switch(config)#arp lock 172.20.0.0/16

8.1.3 arp static

命令

arp static {<ip-prefix> | all}
no arp static

模式

全局配置模式

参数

ip-prefix：IP 地址段，格式 A.B.C.D/M。
all：所有的动态 arp 表项。

描述

对 arp 表项操作。

举例

#将所有动态 arp 表项设置为静态表项：
Switch(config)#arp static all
Switch(config)#

8.1.4 show arp

命令

show arp [<ip-address> | dynamic | lock | static]

模式

普通模式/特权模式

参数

ip-address: ip地址段。
dynamic：动态学习到的arp表。

lock：锁定的arp表信息。

static：静态 arp 表。

描述

显示地址解析表。

举例

显示动态学习到的arp表：

Switch#show arp dynamic

ARP TABLE		
InternetAddress	Physical Address	Type

210.21.223.113	0001.30ba.9c00	dynamic
210.21.223.117	0005.6401.22ad	dynamic

Total Number: 2		

8.1.5 ip prefix-list

命令

ip prefix-list <prefix-list> [seq <seq-num>] {deny | permit} {any | <ip-prefix> [ge <min-len> | le <max-len>]}

no ip prefix-list <prefix-list> [seq <seq-num>] {deny | permit} {any | <ip-prefix> [ge <min-len> | le <max-len>]}

模式

全局配置模式

参数

prefix-list：前缀列表名。

seq-num：前缀列表的序号。

deny：指定匹配模式为拒绝。

permit：指定匹配模式为允许。

any：拒绝/允许所有网络。

ip-prefix：指定拒绝/允许的网络。使用网络/掩码形式表示。

min-len：匹配的最小前缀长度，取值大于掩码长度。

max-len：匹配的最大前缀长度，取值大于或等于 min-len。

描述

ip prefix-list命令用来配置一条前缀列表。

no ip prefix-list命令用来删除一条前缀列表。

举例

#配置一条名为 limit，序号为 15 的前缀列表，拒绝 200.1.1.0/24 的网络：

```
Switch(config)#ip prefix-list limit seq 15 deny 200.1.1.0/24
```

```
Switch(config)#
```

8.1.6 ip route

命令

```
ip route {<ip-address>/<mask-length> | <ip-address> <mask>} <gateway >  
no ip route {<ip-address>/<mask-length> | <ip-address> <mask>}  
[<gateway >]
```

模式

全局配置模式

参数

ip-address：目的 IP 地址，32 位点分十进制格式。

mask-length：掩码长度，十进制表示。

mask：IP 地址的掩码，点分十进制格式。

gateway：指定路由的下一跳网关的IP 地址，点分十进制格式。

描述

ip route命令用来配置静态路由。

no ip route命令用来删除静态路由，在存在多条到达同一网络的路由时，不指定网关将删除所有与目的网络匹配的静态路由。

举例

#配置一条到 210.1.1.0/24 网段的路由，下一跳为 172.20.2.2

```
Switch#configure terminal
```

```
Switch(config)#ip route 210.1.1.0/24 172.20.2.2
```

#删除一条静态路由

```
Switch#configure terminal
```

```
Switch(config)#no ip route 210.1.1.0/24
```

```
Switch(config)#
```


8.1.7 match interface

命令

```
match interface <if-name>  
no match interface [<if-name>]
```

模式

route-map 配置模式

参数

if-name：指定需要匹配的接口名。

描述

match interface命令用来配置一条以接口名为基础的匹配条件。
no match interface命令用来删除一条以接口名为基础的匹配条件。

举例

```
#配置一条规则，匹配条件为接口 vlan55  
Switch(config-route-map)#match interface vlan55  
Switch(config-route-map)#
```

8.1.8 match ip

命令

```
match ip {<ip-address> | <next-hope>} {<acl> | prefix-list <prefix-list>}  
no match ip {<ip-address> | <next-hope>} [<acl> | prefix-list <prefix-list>]
```

模式

route-map 配置模式

参数

ip-address：指定需要匹配路由的 ip 地址。
next-hope：指定需要匹配路由的下一跳地址。
acl：匹配条件需要调用的 acl 规则。
prefix-list：匹配条件需要调用的前缀列表名。

描述

match ip命令用来配置一条以ip地址为基础的匹配条件。
no match ip命令用来删除一条以ip地址为基础的匹配条件。

举例

```
#配置一条规则，匹配条件为下一跳满足前缀列表permitnext的条件：  
Switch(config-route-map)#match ip next-hop prefix-list permitnext
```

Switch(config-route-map)#

8.1.9 match metric

命令

match metric <metric>
no match metric [<metric>]

模式

route-map 配置模式

参数

metric : 路由的花销。

描述

match metric命令用来配置一条以路由metric值为基础的匹配条件。
no match metric命令用来删除一条以路由metric值为基础的匹配条件。

举例

#配置一条规则，匹配条件为路由的 metric 值为 3：
Switch(config-route-map)#match metric 3
Switch(config-route-map)#

8.1.10 match route -type

命令

match route-type external {type-1 | type-2}
no match route-type external [type-1 | type-2]

模式

route-map 配置模式

参数

type-1 : 类型 1 的 ospf 外部路由。
type-2 : 类型 2 的 ospf 外部路由。

描述

match route-type external命令用来配置一条以路由类型为匹配条件的匹配规则，该规则对ospf外部路由有效。
no match route-type external命令用来删除一条以路由类型为匹配条件的匹配规则。

举例

#配置一条规则，匹配条件为 ospf 类型 1 的路由：

```
Switch(config-route-map)#match match route -type external type-1
```

```
Switch(config-route-map)#
```

8.1.11 match tag**命令**

```
match tag <tag>
```

```
no match tag [<tag>]
```

模式

route-map 配置模式

参数

tag：ospf 外部路由的标记值。

描述

match tag命令用来配置一条以路由tag值为匹配条件的匹配规则，该规则对 ospf外部路由有效。

no match tag命令用来删除一条以路由tag值为匹配条件的匹配规则。

举例

#配置一条规则，匹配条件为 ospf 外部路由中 tag 值为 3 的路由：

```
Switch(config-route-map)#match match tag 3
```

```
Switch(config-route-map)#
```

8.1.12 router-id**命令**

```
router-id <router-id>
```

```
no router-id [router-id]
```

模式

全局配置模式

参数

router-id：需要指定的路由器标识，采用 32 位点分十进制格式。

描述

router-id 命令用来配置路由管理中的路由器ID。一些动态路由协议要求使用

路由器ID，如果在启动这些路由协议时没有显示指定路由器ID，则缺省使用路由管理的路由器ID。

no router-id 命令用来删除已配置的路由器ID。

举例

#配置交换机的 router-ID 为 1.1.1.1

Switch(config)#router-id 1.1.1.1

Switch(config)

#删除交换机配置的 router-id

Switch(config)#no router-id

Switch(config)

缺省情况下，路由管理的路由器ID 是0.0.0.0。

8.1.13 route-map

命令

route-map <map-tag> {permit | deny} <sequence>

no route-map <map-tag> {permit | deny} <sequence>

模式

全局配置模式

参数

map-tag：route-map 名。

permit：允许通过。

deny：拒绝通过。

sequence：匹配顺序号。

描述

route-map命令用来创建route-map规则并进入该规则的配置模式下，配置后的route-map规则可以供rip，ospf等协议调用对路由进行控制。

no route-map命令用来删除一组route-map规则中的一条或全部。

举例

#为 route-map“lenovo12800”增加顺序号为 10 的允许通过的规则

Switch(config)#route-map lenovo 12800 permit 10

Switch(config-route-map)#

8.1.14 set ip

命令

```
set ip next-hope <ip-address>
no set ip next-hope [<ip-address>]
```

模式

route-map 配置模式

参数

ip-address：路由的下一跳地址。

描述

set ip命令用来设置符合条件的路由的ip属性。
no set ip命令用来取消对符合条件的路由的ip属性设置。

举例

```
#将符合匹配条件的路由的下一跳设置为 172.20.1.2 :
Switch(config-route-map)#set ip next-hop 172.20.1.2
Switch(config-route-map)#
```

8.1.15 set metric

命令

```
set metric {+/-<metric> | <metric>}
no set metric [+/-<metric> | <metric>]
```

模式

route-map 配置模式

参数

metric：路由的花销值。

描述

set metric命令用来设置符合条件的路由的metric值。
no set metric命令用来取消设置符合条件的路由的metric值。

举例

```
#将符合匹配条件的路由的 metric 值增加 2 :
Switch(config-route-map)#set metric +2
Switch(config-route-map)#
```

8.1.16 set metric-type

命令

```
set metric-type {type-1 | type-2}
no set metric-type [type-1 | type-2]
```

模式

route-map 配置模式

参数

type-1：类型 1 的 ospf 外部路由。
type-2：类型 2 的 ospf 外部路由。

描述

set metric-type命令用来改变符合条件的路由的类型。
no set metric-type命令用来取消对路由类型的改变。

举例

```
#将符合匹配条件的 ospf 外部路由属性改变为 type-1 :
Switch(config-route-map)#set metric-type type-1
Switch(config-route-map)#
```

8.1.17 set tag

命令

```
set tag <tag>
no set tag [<tag>]
```

模式

route-map 配置模式

参数

tag：ospf 外部路由的标记值。

描述

set tag命令用来设置符合匹配条件的路由tag值。
no set tag命令用来取消对路由tag值的设置。

举例

```
#设置符合条件的路由的 tag 值为 10 :
Switch(config-route-map)#set tag 10
Switch(config-route-map)#
```

8.2 显示命令

8.2.1 show ip prefix-list

命令

show ip prefix-list [<prefix-list>] [detail] [summary]

模式

特权模式/普通模式

参数

缺省：显示所有的前缀列表信息。

prefix-list：前缀列表名。

detail：详细信息。

summary：概要信息。

描述

show ip prefix-list命令用来显示前缀列表的相关配置信息。

举例

#查看前缀列表的详细信息：

Switch#show ip prefix-list detail

Prefix-list with the last deletion/insertion: limit

ip prefix-list limit:

count: 1, range entries: 0, sequences: 15 - 15

Switch#

8.2.2 show ip route

命令

show ip route [<network>]

模式

特权模式/普通模式

参数

缺省参数：显示当前路由表中激活的路由。

network：指定显示相关网络的路由，使用 32 位点分十进制或地址前缀/掩码形式表示。

描述

show ip rout 命令用来显示路由信息。内容包括目的地址、掩码长度、协议、优先级、权值、下一跳和输出接口。

该命令只显示当前激活的路由（最佳路由）。

举例

#显示当前使用的路由

Switch#show ip route

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type

2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default

```
R      1.0.0.0/24 [120/2] via 172.20.1.3, vlan2, 00:00:19
R      1.0.1.0/24 [120/2] via 172.20.1.3, vlan2, 00:00:19
R      1.0.2.0/24 [120/2] via 172.20.1.3, vlan2, 00:00:19
C      172.20.1.0/24 is directly connected, vlan2
C      172.20.2.0/24 is directly connected, vlan3
O      172.21.0.128/25 [110/12] via 172.20.2.3, vlan3, 00:00:14
O      172.21.1.0/24 [110/12] via 172.20.2.3, vlan3, 00:00:14
O IA   172.21.2.0/24 [110/20] via 172.20.2.3, vlan3, 00:00:14
O IA   172.21.3.0/24 [110/20] via 172.20.2.3, vlan3, 00:00:14
O E1   172.21.4.0/24 [110/1010] via 172.20.2.3, vlan3, 00:00:14
O E1   172.21.5.0/24 [110/1010] via 172.20.2.3, vlan3, 00:00:14
S      192.1.1.0/24 [1/0] via 172.20.2.2, vlan3
S      200.1.1.0/24 [1/0] via 172.20.1.2, vlan2
```

Switch#

#显示指定网络的路由

Switch#show ip route 1.0.2.0

Routing entry for 1.0.2.0/24

Known via "rip", distance 120, metric 2, best

Last update 00:05:37 ago

* 172.20.1.3, via vlan2

Switch#

Switch#show ip route 1.0.2.1/24

Routing entry for 1.0.2.0/24

Known via "rip", distance 120, metric 2, best

Last update 04:10:29, via vlan2

Switch#

8.2.3 show ip route connected

命令

show ip route connected [count]

模式

特权模式/普通模式

参数

缺省参数：显示当前路由表中激活的直接路由。

count：显示当前激活的直接路由的条数。

描述

show ip rout connected命令用来显示直接路由信息。内容包括目的地址、掩码长度、协议和输出接口。

*该命令只显示当前激活的路由。

举例

#显示当前直接路由

Switch#show ip route connected

C 172.20.1.0/24 is directly connected, vlan2

C 172.20.2.0/24 is directly connected, vlan3

Switch#

#显示当前直接路由条数

Switch#show ip route connected count

total routes: 2

Switch#

8.2.4 show ip route database

命令

show ip route database [<protocol>]

模式

特权模式/普通模式

参数

缺省参数：显示路由表中的所有路由，包括激活和未激活路由。

protocol：跟参数 bgp/connected/isis/ospf/rip/static，显示指定协议的路由。

描述

show ip rout database命令用来整个路由表中的路由信息，包括非激活的路由。

举例

#显示所有的路由

Switch#show ip route database

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type

2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

> - selected route, * - FIB route, p - stale info

R *> 1.0.0.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22

R *> 1.0.1.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22

R *> 1.0.2.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22

C *> 172.20.1.0/24 is directly connected, vlan2

O 172.20.2.0/24 [110/10] is directly connected, vlan3, 04:43:19

C *> 172.20.2.0/24 is directly connected, vlan3

O *> 172.21.0.128/25 [110/12] via 172.20.2.3, vlan3, 04:36:17

O *> 172.21.1.0/24 [110/12] via 172.20.2.3, vlan3, 04:36:17

O IA *> 172.21.2.0/24 [110/20] via 172.20.2.3, vlan3, 04:36:17

O IA *> 172.21.3.0/24 [110/20] via 172.20.2.3, vlan3, 04:36:17

O E1 *> 172.21.4.0/24 [110/1010] via 172.20.2.3, vlan3, 04:36:17

```
O E1 *> 172.21.5.0/24 [110/1010] via 172.20.2.3, vlan3, 04:36:17
S   *> 192.1.1.0/24 [1/0] via 172.20.2.2, vlan3
      >                [1/0] via 172.20.2.4, vlan3
S   *> 200.1.1.0/24 [1/0] via 172.20.1.2, vlan2
```

Switch#

#显示所有的静态路由

Switch#show ip route database static

```
S   *> 192.1.1.0/24 [1/0] via 172.20.2.2, vlan3
      >                [1/0] via 172.20.2.4, vlan3
S   *> 200.1.1.0/24 [1/0] via 172.20.1.2, vlan2
```

Switch#

8.2.5 show route -map

命令

show routemap

模式

特权模式/普通模式

参数

无。

描述

show route-map命令用来显示route-map的配置信息前缀列表的相关信息。

举例

#查看当前 route-map 的配置信息：

Switch#show routemap

route-map lenovo 12800, permit, sequence 10

Match clauses:

Set clauses:

metric-type type-1

tag 10

route-map lenovo 12800, deny, sequence 15

Match clauses:

Set clauses:

Switch#

第 9 章 RIP 命令

9.1 配置命令

9.1.1 default-information originate

命令

default-information originate
no default-information originate

模式

rip 配置模式

参数

无

描述

default-information originate命令用来启动rip协议产生缺省路由并向其他路由器扩散。

no default-information originate命令用来禁止本地rip产生缺省路由。

举例

#启动 rip 产生缺省 rip 路由的功能
Switch(config-rip)#default-information originate
Switch(config-rip)#

9.1.2 default-metric

命令

default-metric <metric>
no default-metric [<metric>]

模式

rip 配置模式

参数

metric：引入路由的缺省花销，取值范围 1~16，默认为 1。

描述

default-metric命令用来指定rip引入路由时的缺省花销。

no default-metric命令用来恢复引入路由的缺省值，恢复metric值为默认值。

举例

```
#配置 rip 引入路由的缺省值为 7
Switch(config-rip)#default-metric 7
Switch(config-rip)#
```

9.1.3 distance

命令

```
distance <distance-value>
no distance [<distance-value>]
```

模式

rip 配置模式

参数

distance-value：指定 rip 路由的管理距离（或称协议优先级）值，取值范围 1 ~ 255。默认值为 120。

描述

distance命令用来指定rip路由的管理距离（协议优先级）。
no distance命令用来删除对管理距离的配置，恢复到默认值。

举例

```
#配置 rip 的管理距离为 100
Switch(config-rip)#distance 100
Switch(config-rip)#
```

9.1.4 distribute-list

命令

```
distribute-list {<acl-name> | prefix [<prefix-list>]} {in | out} [<if-name>]
no distribute-list {<acl-name> | prefix [<prefix-list>]} {in | out} [<if-name>]
```

模式

rip 配置模式。

参数

acl-name：访问控制列表名。
prefix-list：前缀列表名。

in：在入接口上使用过滤。

out：在出接口上使用过滤。

if-name：指定使用过滤功能的接口，缺省为所有启动 RIP 协议的接口。

描述

istribute-list命令用来配置使用访问控制列表和前缀列表在输入输出接口上过滤路由。

no distribute-list命令用来取消路由过滤的配置。

举例

#配置在接口 vlan3 上使用名为 list123 的访问控制列表过滤进入的路由

```
Switch(config-rip)#distribute-list list123 in vlan3
```

```
Switch(config-rip)#
```

9.1.5 ip rip authentication

命令

```
ip rip authentication {mode <mode> | key-chain <key-chain> | string  
<string>}
```

```
no ip rip authentication [mode <mode> | key-chain <key -chain> | string  
<string>]
```

模式

接口配置模式。

参数

mode：认证的方式，取值为 md5 方式和 text（简单文本方式）。

key-chain：key-chainming，配置后调用对应 key-chain 中配置的认证码。

string：认证码，字符串形式，不超过 16 个字符。

描述

ip rip authentication命令用来使能接口对RIP报文的认证功能并配置相关参数。

no ip rip authentication命令用来取消接口对RIP报文的认证功能或修改和删除相关参数。

举例

#配置接口 vlan55 上运行 RIP 协议时使用认证功能，认证方式为 md5，认证密码为 pass123。

```
Switch(config-vlan55)#ip rip authentication mode md5
```

```
Switch(config-vlan55)#ip rip authentication string pass123
Switch(config-vlan55)#
```

9.1.6 ip rip metric

命令

```
ip rip metric <metric>
no ip rip metric [<metric>]
```

模式

接口配置模式。

参数

metric : metric 值，取值范围 1 ~ 16。

描述

ip rip metric 命令用来配置接口接收 RIP 路由时的 metric 值的增量 缺省为 1。
no ip rip metric 命令用来取消对入接口 metric 增量的配置，恢复到默认值。

举例

```
#配置接口 vlan55 上发送 RIP 路由时 metric 值增加 3。
Switch(config-vlan55)#ip rip metric 3
Switch(config-vlan55)#
```

9.1.7 ip rip receive version

命令

```
ip rip receive version <version>
no ip rip receive version [<version>]
```

模式

接口配置模式。

参数

version : 允许接收的 RIP 报文的版本，取值为 1, 2 或 1 2, 即两者皆可。缺省为 2。

描述

ip rip receive version 命令用来配置接口接收 RIP 报文的版本。
no ip rip receive version 命令用来恢复接口接收 RIP 报文的版本为缺省值。

举例

#配置接口 vlan55 上允许接收版本号为 1 的 RIP 报文。

```
Switch(config-vlan55)#ip rip receive version 1
```

```
Switch(config-vlan55)#
```

9.1.8 ip rip receive-packet

命令

```
ip rip receive-packet
```

```
no ip rip receive-packet
```

模式

接口配置模式。

参数

无。

描述

ip rip receive-packet 命令用来使能接口接收 RIP 报文。

no ip rip receive-packet 命令用来配置接口不能接收 RIP 报文。

举例

#配置接口 vlan55 上允许接收 RIP 报文。

```
Switch(config-vlan55)# ip rip receive-packet
```

```
Switch(config-vlan55)#
```

#配置接口 vlan55 上不能接收 RIP 报文

```
Switch(config-vlan55)#no ip rip receive-packet
```

```
Switch(config-vlan55)#
```

9.1.9 ip rip send version

命令

```
ip rip send version < version>
```

```
no ip rip send version [<version>]
```

模式

接口配置模式。

参数

version：允许发送的 RIP 报文的版本，取值为 1 或 2。缺省为 2。

描述

ip rip send version 命令用来配置接口发送 RIP 报文的版本。

no ip rip send version 命令用来恢复接口发送 RIP 报文的版本为缺省值。

举例

#配置接口 vlan55 上允许发送版本号为 1 的 RIP 报文。

```
Switch(config-vlan55)#ip rip send version 1
```

```
Switch(config-vlan55)#
```

9.1.10 ip rip send -packet

命令

```
ip rip send -packet
```

```
no ip rip send -packet
```

模式

接口配置模式。

参数

无。

描述

ip rip send -packet 命令用来使能接口发送 RIP 报文。

no ip rip send -packet 命令用来配置接口不能发送 RIP 报文。

举例

#配置接口 vlan55 上允许发送 RIP 报文。

```
Switch(config-vlan55)# ip rip send -packet
```

```
Switch(config-vlan55)#
```

#配置接口 vlan55 上不能发送 RIP 报文

```
Switch(config-vlan55)#no ip rip send -packet
```

```
Switch(config-vlan55)#
```

9.1.11 ip rip split-horizon

命令

```
ip rip split-horizon [poisoned]
```

```
no ip rip split-horizon
```

模式

接口配置模式。

参数

poisoned：带毒性逆转的水平分割方式。

描述

ip rip split-horizon 命令用来使能接口上的水平分割功能。缺省情况为带毒性逆转的水平分割方式。

no ip rip split-horizon 命令用来配置接口上不使用水平分割功能。

举例

#配置接口 vlan55 上使能带毒性逆转的水平分割。

```
Switch(config-vlan55)# ip rip split-horizon poisoned
```

```
Switch(config-vlan55)#
```

9.1.12 maximum-prefix

命令

```
maximum-prefix <max-num> [<waring-num>]
```

```
no maximum -prefix [<max-num>] [<waring-num>]
```

模式

rip 配置模式。

参数

max-num : RIP 路由的最大条数, 取值范围 1 ~ 65535。

waring-num : 发出路由报警的百分比, 取值范围 1 ~ 100。

描述

maximum-prefix命令用来配置路由表容量及告警容限。

no maximum -prefix命令用来取消对路由表的容量限制和告警配置。

举例

#配置 RIP 路由上限为 1000 条, 达到 60%时发出告警

```
Switch(config-rip)#maximum -prefix 1000 60
```

```
Switch(config-rip)#
```

9.1.13 neighbor

命令

```
neighbor <neighbor-address>
```

```
no neighbor <neighbor-address>
```

模式

rip 配置模式。

参数

neigubor-address : 邻居的 ip 地址 , 点分 10 进制格式。

描述

neighbor 命令为RIP在非广播网络上指定邻居。

no neighbor命令取消指定邻居。

举例

#指定邻居 10.80.50.111

Switch(config-rip)#neighbor 10.80.50.111

Switch(config-rip)#

9.1.14 network**命令**

network {<ip-prefix>/<mask-length> | < ip-prefix > <mask>}

no network {<ip-prefix>/<mask-length> | < ip-prefix > <mask>}

模式

rip 配置模式。

参数

ip-prefix : ip 地址前缀。

mask-length : 10 进制掩码长度。

mask : 32 位点分 10 进制掩码。

描述

network命令用来使能一个子网运行RIP协议。

no network命令用来禁止一个子网使能RIP协议。

举例

#指定子网 192.168.1.0/24 运行 RIP 协议

Switch(config-rip)#network 192.168.1.0/24

Switch(config-rip)#

9.1.15 offset-list**命令**

offset-list <acl-name> {in | out} <metric> [<if-name>]

no offset-list <acl-name> {in | out} <metric> [<if-name>]

模式

rip 配置模式。

参数

acl-name：调用的访问控制列表名。

in：在入接口上应用。

out：在出接口上应用。

metric：路由 metric 值的偏移量。

if-name：应用该规则的接口，缺省为所有接口。

描述

offset-list 命令用来配置 RIP 通过 ACL 过滤对接口输入或输出的路由增加一定的偏移值。

no offset-list 命令用来取消特定路由的偏移增量配置。

举例

#对通过名为“list123”的访问控制列表过滤的路由出接口 vlan3 上 metric 值增加 3

```
Switch(config-rip)#offset-list list123 out 3 vlan3
```

```
Switch(config-rip)#
```

9.1.16 passive-interface

命令

```
passive-interface <if-name>
```

```
no passive-interface <if-name>
```

模式

rip 配置模式。

参数

if-name：指定接口。

描述

passive-interface 命令用来配置接口为被动接口，配置后接口能够接收 RIP 报文，但不能发送 RIP 报文。

no passive-interface 命令用来恢复接口为可收发状态。

举例

#配置接口 vlan3 为被动接口

```
Switch(config-rip)#passive-interface vlan3
```

Switch(config-rip)#

9.1.17 recv-buffer-size

命令

recv-buffer-size <buffer-size>
no recv-buffer-size [<buffer-size>]

模式

rip 配置模式。

参数

buffer-size：接收缓冲区大小值，取值范围 8192~ 2147483647。

描述

recv-buffer-size 命令用来配置 RIP 报文接收缓冲区的大小。
no recv-buffer-size 命令用来取消对 RIP 接收缓冲区大小的指定

举例

```
#配置接收缓冲区大小为 102400
Switch(config-rip)# recvbuffer-size 102400
Switch(config-rip)#
```

9.1.18 redistribute

命令

redistribute <protocol> [metric <metric>] [route-map <route-map>]
no redistribute <protocol> [metric <metric>] [route-map <route-map>]

模式

rip 配置模式。

参数

protocol:需要引入到 RIP 中的路由协议类型如 is-is ,ospf ,bgp ,static ,connect 等。

metric：指定引入路由时的 metric 值。

route-map：引入路由时需要引用的 route-map 名。

描述

redistribute 用来引入其他协议的路由到 RIP 中。
no redistribute 用来取消对其他协议路由的引入。缺省情况下不做引入。

举例

#引入直连路由到 RIP 路由表中，并通过 route-map 规则“list123”规则，指定引入路由的 metric 值为 9。

```
Switch(config-rip)#redistribute connected metric 9 route-map list123
Switch(config-rip)#
```

9.1.19 route

命令

```
route <network>/<mask-length>
no route <network>/<mask-length>
```

模式

rip 配置模式。

参数

network：路由的目的网络。

mask-length：目的网络的掩码长度。

描述

route 命令用来增加一条静态路由到 RIP 路由表中，再 RIP 域内扩散该路由。

no route 命令用来取消一条加入到 RIP 中的静态路由。

举例

```
#增加一条到目的网络 200.1.1.0/24 的静态路由到 RIP 路由表中
Switch(config-rip)# route 200.1.1.0/24
Switch(config-rip)#
```

9.1.20 router rip

命令

```
router rip
no router rip
```

模式

全局配置模式

参数

无

描述

router rip命令用来启动rip协议并进入rip配置模式。

no router rip命令用来关闭rip协议，并删除配置。

举例

#启动并进入 rip 配置模式

Switch(config)#router rip

Switch(config-rip)#

9.1.21 timers

命令

timers basic <update-interval> <dead-interval> <garbage-interval>

no timers basic

模式

rip 配置模式。

参数

update-interval：发送 RIP 周期性更新报文的时间间隔。默认为 30 秒。

dead-interval：没有得到更新的被设置为不可用的 RIP 路由的等待时间。默认为 180 秒。

garbage-interval：从 RIP 路由设置为不可用到彻底从路由表中删除的时间间隔。默认为 120 秒。

描述

timers basic 命令用来配置与 RIP 相关的定时器值。

no timers basic 命令用来恢复 RIP 定时器到缺省值。

举例

#配置 RIP 协议的周期性更新时间为 20 秒，死亡时间为 100 秒，垃圾收集时间为 60 秒。

Switch(config-rip)#timers basic 20 100 60

Switch(config-rip)#

9.1.22 version

命令

version <version>

no version [<version>]

模式

rip 配置模式。

参数

version : RIP 的版本，取值范围：1 ~ 2。

描述

version 命令用来指定 RIP 协议的版本，默认值为 2。

no version 命令用来恢复到系统默认的版本。

举例

#配置 RIP 协议的版本为版本 1。

```
Switch(config-rip)#version 1
```

```
Switch(config-rip)#
```

9.2 查看命令

9.2.1 show ip rip

命令

```
show ip rip [database[count] / interface [<if-name>]]
```

模式

特权模式/普通模式。

参数

缺省：显示当前系统 rip 的相关信息。

database：查看 rip 路由信息数据库。

count：显示 rip 路由信息数据库中的条数。

interface：查看启动了 rip 协议的接口相关信息。

if-name：查看指定接口上的 rip 相关信息

描述

show ip rip 命令用来显示当前的 rip 信息。

举例

#显示接口 vlan51 上当前的 rip 配置。

```
Switch#show ip rip interface vlan51
```

```
vlan51 is up, line protocol is up
```

```
Routing Protocol: RIP
```



```
Receive RIP packets
Send RIP packets
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
    172.20.6.2/24
```

Switch#

9.2.2 show ip route rip

命令

```
show ip route rip [count]
```

模式

特权模式/普通模式。

参数

缺省：显示当前激活的 rip 路由。

count：显示当前激活的 rip 路由的条数。

描述

show ip route rip 命令用来显示当前激活的 rip 路由信息。

举例

#显示当前激活的 rip 路由。

```
Switch#show ip route rip
```

```
R    1.0.0.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22
```

```
R    1.0.1.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22
```

```
R    1.0.2.0/24 [120/2] via 172.20.1.3, vlan2, 04:36:22
```

```
Switch#
```

#显示当前激活的 rip 路由的条数。

```
Switch#show ip rout rip count
```

```
total routes: 3
```

```
Switch#
```

9.2.3 show running rip

命令

show running rip

模式

特权模式/普通模式。

参数

无。

描述

show running rip 命令用来显示当前的 RIP 配置。

举例

#显示当前的 rip 配置。

Switch#show running-config rip

!

router rip

network 172.20.13.0/24

network 172.20.14.0/24

!

Switch#

9.3 调试命令

9.3.1 debug rip

命令

debug rip

no debug rip

模式

特权模式。

参数

无。

描述

debug rip 命令用来打开当前 rip 的调试开关 ,使用户能够看到 rip 的协商过程和报文收发情况。

no debug rip 命令用来关闭 rip 的调试开关。

举例

#打开 rip 的调试开关：

```
Switch#debug rip
```

```
Switch#
```

9.3.2 debug rip all

命令

```
debug rip all
```

```
no debug rip all
```

模式

特权模式。

参数

无。

描述

debug rip all 命令用来打开所有 rip 相关的调试开关，使用户能够看到 rip 的协商过程和报文收发情况。

no debug rip all 命令用来关闭所有 rip 相关的调试开关。

举例

#打开 rip 相关的所有调试开关：

```
Switch#debug rip packet all
```

```
Switch#
```

9.3.3 debug rip events

命令

```
debug rip events
```

```
no debug rip events
```

模式

特权模式。

参数

无。

描述

debug rip events 命令用来打开 rip 的事件调试开关，使用户能够看到 rip 的协商过程。

no debug rip events 命令用来关闭 rip 的事件调试开关。

举例

#打开 rip 的事件调试开关：

```
Switch#debug rip events
```

```
Switch#
```

9.3.4 debug rip packet

命令

```
debug rip packet [recv | send] [detail]
```

```
no debug rip packet [recv | send] [detail]
```

模式

特权模式。

参数

recv：打开接收报文调试开关。

send：打开发送报文调试开关。

detail：打开 rip 报文的详细信息调试开关。

描述

debug rip packet 命令用来打开 rip 报文调试开关，使用户能够看到 rip 报文收发情况。

no debug rip packet 命令用来关闭 rip 报文调试开关。

举例

#打开 rip 的接收报文详细信息调试开关：

```
Switch#debug rip packet recv detail
```

```
Switch#
```

第 10 章 OSPF 命令

10.1 配置命令

10.1.1 area authentication

命令

```
area <area-id> authentication [message-digest]
no area <area-id> authentication
```

模式

ospf 配置模式。

参数

area-id : ospf 区域 id，可以十进制表示，取值范围 0 ~ 4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0~ 255.255.255.255。

message-digest : 指定使用 MD5 密文验证。若无参数则使用明文认证。

描述

area <area-id> authentication 命令用来配置区域使用验证，并指定验证方式。

no area <area-id> authentication 命令用来取消区域验证功能。

举例

#配置 ospf 进程 11 的区域 1 使用 MD5 验证：

```
Switch(config-ospf-11)#area 1 authentication message-digest
Switch(config-ospf-11)#
```

10.1.2 area default-cost

命令

```
area <area-id> default-cost <cost>
no area <area-id> default-cost
```

模式

ospf 配置模式。

参数

area-id : ospf 区域 id，可以十进制表示，取值范围 0 ~ 4294967295；也可以

是 32 位的点分十进制表示。取值范围为 0.0.0.0~ 255.255.255.255。

cost：路由花销值，取值范围 0 ~ 16777214。

描述

area <area-id> default-cost 命令用来配置从 ABR 发送到 stub 区域和 nssa 区域的 summary 路由的缺省代价。

no area <area-id> default-cost 命令用来取消区域的缺省花销配置，恢复到默认值。

举例

#配置区域 1 的默认 cost 为 224：

```
Switch(config-ospf-11)#area 1 default-cost 224
```

```
Switch(config-ospf-11)#
```

10.1.3 area filter-list

命令

area <area-id> filter-list {access <access-list> | prefix <prefix-list>} {in | out}

no area <area-id> filter-list {access <access-list> | prefix <prefix-list>} {in | out}

模式

ospf 配置模式。

参数

area-id：ospf 区域 id，可以十进制表示，取值范围 0 ~ 4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0~ 255.255.255.255。

access access-list：访问控制列表名。

prefix prefix-list：地址前缀列表名。

in：指定为入方向有效。

out：指定为出方向有效。

描述

area <area-id> filter-list 命令用来在 ABR 上配置过滤器，可使用 access list 也可使用 prefix list 过滤 summary 路由，in 为灌入本 area 的方向，out 为本 area 广播出去的方向。

no area <area-id> filter-list 命令用来取消在 ABR 上对区域 summary 路由进行过滤。

举例

#配置 ospf 进程 11 的区域 1 的 ABR 上使用名为 list123 的前缀列表对收到的路由进行过滤：

```
Switch(config-ospf-11)#area 1 filter-list prefix list123 in
Switch(config-ospf-11)#
```

10.1.4 area nssa

命令

```
area <area-id> nssa [default-information-originate] [no-redistribution]
[no-summary] [translator-role]
no area <area-id> nssa [default-information-originate] [no-redistribution]
[no-summary] [translator-role]
```

模式

ospf 配置模式。

参数

area-id : ospf 区域 id，可以十进制表示，取值范围 0 ~ 4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0~ 255.255.255.255。

default-information-originate :生成一条类型为 7 的缺省路由发向 nssa 区域。

no-redistribution : 指定该 nssa 区域不能使用路由引入。

no-summary : 配置 ABR 不发送 summary 类型的 LSA 到 NSSA 区域内。

translator-role : 指定为 nssa 区的 ABR。

描述

area <area-id> nssa 命令用来配置区域为 nssa 区域，并可同时指定相关参数。

no area <area-id> nssa 命令用来恢复区域为普通区域或删除 nssa 区域的参数。

举例

#配置 ospf 进程 11 的区域 1 为 nssa 区域，路由器生成一条类型 7 的缺省路由，ABR 不扩散 summaryLSA 到 nssa 区域内：

```
Switch(config-ospf-11)#area 1 nssa default-information-originate
no-summary
Switch(config-ospf-11)#
```

10.1.5 area range

命令

```
area <area-id> range <ip-prefix> [advertise | not-advertise]
no area <area-id> range <ip-prefix> [advertise | not-advertise]
```

模式

ospf 配置模式。

参数

area-id : ospf 区域 id，可以十进制表示，取值范围 0 ~ 4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0 ~ 255.255.255.255。

ip-prefix : 聚合的路由范围，网络/掩码格式。

advertise : 聚合后通告聚合的路由。

not-advertise : 不通告聚合的路由。

描述

area <area-id> range 命令用来配置区域内的路由聚合或附加参数。

no area <area-id> range 命令用来取消区域的路由聚合或删除附加参数。

举例

#配置 ospf 进程 11 的区域 1 进行路由聚合，并通过聚合后的路由：

```
Switch(config-ospf-11)#area 1 range 1.1.1.1/8 advertise
```

```
Switch(config-ospf-11)#
```

10.1.6 area shortcut

命令

```
area <area-id> shortcut [default | disable | enable]
no area <area-id> shortcut [default | disable | enable]
```

模式

ospf 配置模式。

参数

area-id : ospf 区域 id，可以十进制表示，取值范围 0 ~ 4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0 ~ 255.255.255.255。

default : 缺省模式。

disable : 禁止。

enable : 强制。

描述

area <area-id> shortcut 命令用来配置 area 的 shortcut 功能，当使能时，数据流可以仅花费较小的代价穿过非骨干区域而无需考虑 ABR 是否连接到骨干区域上。

no area <area-id> shortcut 命令用来取消区域的 shortcut 配置。

举例

#配置 ospf 进程 11 的区域 1 的 shortcut 功能：

```
Switch(config-ospf-11)#area 1 shortcut enable
```

```
Switch(config-ospf-11)#
```

10.1.7 area stub

命令

```
area <area-id> stub [no-summary]
```

```
no area <area-id> stub [no-summary]
```

模式

ospf 配置模式。

参数

area-id : ospf 区域 id，可以十进制表示，取值范围 0 ~ 4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0~ 255.255.255.255。

no-summary :配置 ABR 不向 stub 区域通告 summary 路由。缺省允许通告。

描述

area <area-id> stub 命令用来指定区域为 stub 区域。

no area <area-id> stub 命令用来取消指定区域为 stub 区域。

举例

#配置 ospf 进程 11 的区域 1 为 stub 区域，不学习 summary 路由：

```
Switch(config-ospf-11)#area 1 stub no-summary
```

```
Switch(config-ospf-11)#
```

10.1.8 area virtual-link

命令

```
area <area-id> virtual-link <neighbor-id> [dead-interval <dead-interval>]
```

```
[hello-interval <hello-interval>] [retransmit-interval <retran-interval>]
```

```
[transmit-delay <delay-interval>]
```

```
no area <area-id> virtual-link <neighbor-id> [dead-interval <dead-interval>]
```

```
[hello-interval <hello-interval>] [retransmit-interval <retran-interval>]
[transmit-delay <delay-interval>]
```

模式

ospf 配置模式。

参数

area-id : ospf 区域 id，可以十进制表示，取值范围 0 ~ 4294967295；也可以是 32 位的点分十进制表示。取值范围为 0.0.0.0~ 255.255.255.255。

neighbor-id : 虚连接对端的路由器 Router-id。

dead-interval : 配置虚连接上路由器失效的死亡时间。缺省为 4 倍 hello 报文周期（40s）。

hello-interval : 配置虚连接上的 hello 报文发送的时间间隔。缺省为 10s。

retran-interval : 配置虚连接上的报文重传时间间隔。缺省为 5s。

delay-interval : 配置虚连接上的报文传输延迟时间。缺省为 40s。

描述

area <area-id> virtual-link 命令用来配置一条虚连接及相关参数。

no area <area-id> virtual-link 命令用来删除虚连接或恢复虚连接上的参数到默认配置。

举例

#配置 ospf 进程 11 的区域 1 里与邻居 1.1.1.1 建立虚连接，hello 时间间隔为 5s：

```
Switch(config-ospf-11)#area 1 virtual-link 1.1.1.1 hello-interval 5
```

```
Switch(config-ospf-11)#
```

10.1.9 area virtual-link authentication**命令**

```
area <area-id> virtual-link <neigubor-id> [authentication]
[authentication-key <key-string>] [message-digest] [message-digest-key
<key-id> md5 <key-string>] [null]
```

```
no area <area-id> virtual-link <neigubor-id> [authentication]
[authentication-key <key-string>] [message-digest] [message-digest-key
<key-id> md5 <key-string>] [null]
```

模式

ospf 配置模式。

参数

neigubor-id：虚连接对端的路由器 Router-id。

area-id：ospf 区域 id，可以十进制表示，取值范围 0 ~ 4294967295；也可以是 32 位的点十进制表示。取值范围为 0.0.0.0~ 255.255.255.255。

authentication：配置虚连接使用认证功能。

authentication-key key-string：配置使用简单验证的验证字。

message-digest：配置使用秘文验证。

message-digest-key key-id md5 key-string：配置使用 md5 秘文验证及验证字的 id 和验证字。

null：不使用验证功能。

描述

area <area-id> virtual-link authentication 命令用来为一条虚连接配置验证功能及相关参数。

no area <area-id> virtual-link authentication 命令用来删除虚连接上的验证或验证的相关参数。

举例

```
#配置 ospf 进程 11 的区域 1 上与邻居 1.1.1.1 建立虚连接使用简单文本验证：
Switch(config-ospf-11)#area 1 virtual-link 1.1.1.1 authentication
authentication-key pass123
Switch(config-ospf-11)#
```

10.1.10 auto-cost reference-bandwidth

命令

auto-cost reference-bandwidth <bandwidth>

no auto-cost reference-bandwidth

模式

ospf 配置模式。

参数

bandwidth：参考带宽，单位为 Mbits/s，取值范围 1 ~ 4294967，缺省为 10000Mbits/s。

描述

auto-cost reference-bandwidth 命令用来配置参考带宽值，ospf 协议根据配置值计算路由的花销。

no auto-cost reference-bandwidth 命令用来删除参考带宽值的配置，恢复到缺省值。

举例

```
#配置 ospf 进程 11 的参考带宽为 1000Mbps/s :
Switch(config-ospf-11)#auto-cost reference-bandwidth 1000
Switch(config-ospf-11)#
```

10.1.11 compatible rfc1583**命令**

```
compatible rfc1583
no compatible rfc1583
```

模式

ospf 配置模式。

参数

无。

描述

compatible rfc1583 命令用来配置本机 ospf 协议兼容 rfc1583。
no compatible rfc1583 命令用来配置本机 ospf 不兼容 rfc1583。

举例

```
#配置 ospf 进程 11 兼容 rfc1583 :
Switch(config-ospf-11)#compatible rfc1583
Switch(config-ospf-11)#
```

10.1.12 default-information originate**命令**

```
default-information originate [always] [metric] [metric-type] [route-map]
no default-information originate [always] [metric] [metric-type] [route-map]
```

模式

ospf 配置模式。

参数

always：总是通告缺省路由。
metric：通告缺省路由的花销。

metric-type：通告缺省路由的类型，取值为 1 或 2，缺省为 2。

route-map：通告缺省路由时调用 route-map 规则。

描述

default-information originate 命令用来配置本地路由器生成一条缺省的 ospf 路由及相关参数，并通告到邻居。

no default-information originate 命令用来取消生成缺省路由或改变相关参数。

举例

#配置 ospf 进程 11 生成一条 metric 为 12 的缺省路由：

```
Switch(config-ospf-11)#default-information originate metric 12
```

```
Switch(config-ospf-11)#
```

10.1.13 default-metric

命令

```
default-metric <metric>
```

```
no default-metric [<metric>]
```

模式

ospf 配置模式。

参数

metric：引入路由的缺省花销，取值范围为 0~16777214，缺省为 1。

描述

default-metric 命令用来配置 ospf 引入路由的缺省 metric 值。

no default-metric 命令用来恢复引入路由的 metric 值为缺省值。

举例

#配置 ospf 进程 11 引入路由的缺省 metric 为 12：

```
Switch(config-ospf-11)#default-metric 12
```

```
Switch(config-ospf-11)#
```

10.1.14 distance

命令

```
distance [<distance> | ospf external <distance> | ospf inter-area <distance> | ospf intra-area <distance>]
```

```
no distance {<distance> | ospf external <distance> | ospf inter-area  
<distance> | ospf intra-area <distance>}
```

模式

ospf 配置模式。

参数

distance: 路由的管理距离, 取值范围 1 ~ 255, 缺省为 110。

external: 通过路由引入获得的外部路由。

inter-area: 区域间路由。

intra-area: 区域内路由。

描述

distance 命令用来配置 ospf 路由的管理距离。

no distance 命令用来恢复 ospf 路由的管理距离到缺省值。

举例

#配置 ospf 路由的管理距离为 120:

```
Switch(config-ospf-11)#distance 120
```

```
Switch(config-ospf-11)#
```

10.1.15 distribute-list

命令

```
distribute-list <acl-list> out <protocol>
```

```
no distribute-list <acl-list> out <protocol>
```

模式

ospf 配置模式。

参数

acl-list: 访问控制列表名。

out: 在向外通告路由时进行过滤。

protocol: 指定过滤实施的目标协议。

描述

distribute-list 命令用来配置 ospf 通告路由时对引入的路由进行过滤。

no distribute-list 命令用来取消路由过滤。

举例

#配置 ospf 通告路由时对引入的 rip 路由使用名为 list123 的 acl 进行过滤:

```
Switch(config-ospf-11)# distributelist list123 out rip
```

```
Switch(config-ospf-11)#
```

10.1.16 host

命令

```
host <host-address> area <area-id> [cost <cost>]  
no host <host-address> area <area-id> [cost <cost>]
```

模式

ospf 配置模式。

参数

host-address：主机地址，32 位点分十进制。

area-id：区域 id，点分十进制 0.0.0.0~ 255.255.255.255 或数字 0~ 4294927695。

cost：路由花销，取值范围 0 ~ 65535。

描述

host 命令用来在一个区域内配置一条主机路由，在 router lsa 中以 stub 类型的 link 广播出去。

no host 命令用来取消主机路由及相关配置。

举例

#配置 ospf 11 的区域 1 中通告一条 172.20.1.1 的主机路由，cost 为 5：

```
Switch(config-ospf-11)#host 172.20.1.1 area 1 cost 5
```

```
Switch(config-ospf-11)#
```

10.1.17 ip ospf authentication

命令

```
ip ospf authentication [message-digest] [null]  
no ip ospf authentication
```

模式

接口配置模式。

参数

缺省：使用简单文本验证。

message-digest：使用密文验证。

null：不使用验证。

描述

ip ospf authentication 命令用来配置配置接口的验证模式。

no ip ospf authentication 命令用来取消接口验证。

举例

#配置接口 vlan5 使用简单文本验证：

Switch(config-vlan5)#ip ospf authentication

Switch(config-vlan5)

10.1.18 ip ospf authentication-key**命令**

ip ospf authentication-key <key-string>

no ip ospf authentication-key

模式

接口配置模式。

参数

key-string：简单文本验证的密码。

描述

ip ospf authentication-key 命令用来配置简单文本验证的密码。

no ip ospf authentication-key 命令用来删除简单文本验证的密码。

举例

#配置接口 vlan5 使用简单文本验证密码“pass123”：

Switch(config-vlan5)#ip ospf authentication-key pass123

Switch(config-vlan5)

10.1.19 ip ospf cost**命令**

ip ospf cost <cost>

no ip ospf cost

模式

接口配置模式。

参数

cost：接口的链路花销，取值范围 1 ~ 65535。

描述

ip ospf cost 命令用来配置接口的链路花销，该值对出接口路由有效。
no ip ospf cost 命令用来恢复接口的链路花销到缺省值。

举例

#配置接口 vlan5 的链路花销为 23：
Switch(config-vlan5)#ip ospf cost 23
Switch(config-vlan5)

10.1.20 ip ospf database-filter**命令**

ip ospf database-filter all out
no ip ospf database-filter

模式

接口配置模式。

参数

all：所有的路由信息。
out：出方向阻塞。

描述

ip ospf database-filter 命令用来配置接口阻塞泛洪。
no ip ospf database-filter 命令用来恢复接口的泛洪功能。

举例

#配置接口 vlan5 不发送 ospf 的 LSA 信息：
Switch(config-vlan5)#ip ospf database-filter all out
Switch(config-vlan5)

10.1.21 ip ospf dead-interval**命令**

ip ospf dead-interval <interval>
no ip ospf dead-interval

模式

接口配置模式。

参数

interval：该接口上 dead 定时器的时间，取值范围 1 ~ 65535，广播网上缺省为 40，单位为秒。

描述

ip ospf dead-interval 命令用来配置接口的 dead 定时器值。

no ip ospf dead-interval 命令用来恢复接口 dead 定时器到缺省值。

举例

#配置接口 vlan5 上 ospf 邻居 dead 时间为 20s：

```
Switch(config-vlan5)# ip ospf dead-interval 20
```

```
Switch(config-vlan5)
```

10.1.22 ip ospf disable all

命令

```
ip ospf disable all
```

```
no ip ospf disable all
```

模式

接口配置模式。

参数

无。

描述

ip ospf disable 禁止该接口所有的功能，不再处理包；该命令优先于 network 命令。

no ip ospf disable 命令用来恢复接口的 ospf 功能。

举例

#配置接口 vlan5 上禁止 ospf 功能：

```
Switch(config-vlan5)# ip ospf disable all
```

```
Switch(config-vlan5)
```

10.1.23 ip ospf hello-interval

命令

```
ip ospf hello-interval <interval>
```

```
no ip ospf hello-interval
```

模式

接口配置模式。

参数

interval：该接口上 hello 定时器的时间间隔，取值范围 1 ~ 65535，缺省为 10，单位为秒。

描述

ip ospf hello-interval 命令用来配置接口的 hello 定时器时间间隔。

no ip ospf hello-interval 命令用来恢复接口 hello 定时器到缺省值。

举例

#配置接口 vlan5 上 ospf 邻居 hello 定时器时间间隔为 5s：

```
Switch(config-vlan5)#ip ospf hello-interval 5
```

```
Switch(config-vlan5)
```

10.1.24 ip ospf message-digest-key

命令

```
ip ospf message-digest-key <key-id> md5 <key-string>
```

```
no ip ospf message-digest-key <key-id>
```

模式

接口配置模式。

参数

key-id：密文认证的 id 号，取值范围 1 ~ 255。

key-string：密文认证的字符串。

描述

ip ospf message-digest-key 命令用来配置接口密文认证的字符串。

no ip ospf message-digest-key 命令用来删除接口密文认证的字符串。

举例

#配置接口 vlan5 上 ospf 的密文认证字 id 为 10，字符串为“123pass”：

```
Switch(config-vlan5)#ip ospf message-digest-key 10 md5 123pass
```

```
Switch(config-vlan5)#
```

10.1.25 ip ospf mtu

命令

```
ip ospf mtu <mtu>
```

no ip ospf mtu

模式

接口配置模式。

参数

mtu：接口最大传输单元，取值范围 576-65535。

描述

ip ospf mtu 命令用来配置接口的最大传输单元。

no ip ospf mtu 命令用来恢复 mtu 到缺省值。

举例

#配置接口 vlan5 上最大传输单元为 1000：

Switch(config-vlan5)# ip ospf mtu 1000

Switch(config-vlan5)#

10.1.26 ip ospf mtu-ignore

命令

ip ospf mtu-ignore

no ip ospf mtu-ignore

模式

接口配置模式。

参数

无。

描述

ip ospf mtu-ignore 命令用来配置接口接收到 DD 报文时的 mtu 忽略功能，接收到报文时不检查 mtu 位。

no ip ospf mtu-ignore 命令用来恢复接口对 mtu 的检查。

举例

#配置接口 vlan5 上不检查 mtu：

Switch(config-vlan5)# ip ospf mtu-ignore

Switch(config-vlan5)#

10.1.27 ip ospf network

命令

```
ip ospf network {broadcast | non-broadcast | point-to-multipoint  
[non-broadcast] | point-to-point}
```

```
no ip ospf network
```

模式

接口配置模式。

参数

broadcast:广播网类型。

non-broadcast：非广播网类型。

point-to-multipoint：点到多点网络类型。

point-to-point：点到点网络类型。

描述

ip ospf network 命令用来指定接口所在的网络类型，ospf 根据不同的网络类型运行对应的 ospf 处理机制。

no ip ospf network 命令用来恢复接口到缺省的网络类型。

举例

#配置接口 vlan5 的网络类型为点到点：

```
Switch(config-vlan5)# ip ospf network point-to-point
```

```
Switch(config-vlan5)#
```

10.1.28 ip ospf priority

命令

```
ip ospf priority <priority>
```

```
no ip ospf priority
```

模式

接口配置模式。

参数

priority：接口优先级，取值范围 0 ~ 255，默认值为 1。

描述

ip ospf priority 命令用来指定接口优先级。

no ip ospf priority 命令用来恢复接口默认优先级。

举例

#配置接口 vlan5 的优先级为 10：

```
Switch(config-vlan5)# ip ospf priority 10
```

Switch(config-vlan5)#

10.1.29 ip ospf retransmit-interval

命令

ip ospf retransmit-interval <interval>
no ip ospf retransmit-interval

模式

接口配置模式。

参数

interval：该接口上 retransmit 定时器的时间，取值范围 1 ~ 65535，缺省为 5，单位为秒。

描述

ip ospf retransmit-interval 命令用来配置接口的重传定时器值。
no ip ospf retransmit-interval 命令用来恢复接口重传定时器到缺省值。

举例

#配置接口 vlan5 上 ospf 的 retransmi 周期时间为 15s：
Switch(config-vlan5)# ip ospf retransmit-interval 15
Switch(config-vlan5)

10.1.30 ip ospf transmit-delay

命令

ip ospf transmit-delay <interval>
no ip ospf transmit-delay

模式

接口配置模式。

参数

interval：该接口上传输延迟时间，取值范围 1 ~ 65535，缺省为 40，单位为秒。

描述

ip ospf transmit-delay 命令用来配置接口的传输延迟值。
no ip ospf transmit-delay 命令用来恢复接口传输延迟到缺省值。

举例

```
#配置接口 vlan5 上 ospf 的传输延迟时间为 25s :  
Switch(config-vlan5)#ip ospf transmit-interval 25  
Switch(config-vlan5)
```

10.1.31 max-concurrent-dd

命令

```
max-concurrent-dd <number>  
no max-concurrent-dd
```

模式

ospf 配置模式。

参数

number : DD 报文数, 取值范围为 1 ~ 65535, 缺省为 5。

描述

max-concurrent-dd 命令用来控制 DD 挂起列表的最大个数。若在 DD 交换过程中出错, 邻居会被放入这个挂起列表。

no max-concurrent-dd 命令用来恢复到缺省值。

举例

```
#配置 ospf 11 的 DD 报文挂起最大数为 100 :  
Switch(config-ospf-11)# max-concurrent-dd 100  
Switch(config-ospf-11)#
```

10.1.32 neighbor

命令

```
neighbor <router-id> [cost <cost>] [poll-interval <interval>] [priority  
<priority>]  
no neighbor <router-id> [cost <cost>] [poll-interval <interval>] [priority  
<priority>]
```

模式

ospf 配置模式。

参数

router-id : 邻居 router-id, 32 位点分十进制。

cost : 链路的花销, 取值范围 1 ~ 65535。

interval : 认为邻居 dead 的时间, 取值范围 1 ~ 65535, 单位为秒。

priority : DR 选举时的优先级, 取值范围 0~ 255。

描述

neighbor 命令用来在 NBMA 网络上指定一个邻居, 并配置相关参数。

no neighbor 命令用来取消 NBMA 网络上指定的一个邻居。

举例

#配置 NBMA 网络上的邻居 1.1.1.2, 协商优先级为 10 :

```
Switch(config-ospf-11)# neighbor 1.1.1.2 priority 10
```

```
Switch(config-ospf-11)#
```

10.1.33 network

命令

```
network <network> area <area-id>
```

```
no network <network> area <area-id>
```

模式

ospf 配置模式。

参数

network : 使能 ospf 的网络, 网络/掩码或网络 + 反向掩码形式。

area-id : 区域 id, 32 位点分十进制或数字形式。

描述

network 命令用来使能一个网络并指定加入的区域。

no network 命令用来取消一个网络的使能。

举例

#配置使能网络 172.20.1.0/24 到 ospf 11 的区域 0 中 :

```
Switch(config-ospf-11)# network 172.20.1.0/24 area 0
```

```
Switch(config-ospf-11)#
```

10.1.34 passive-interface

命令

```
passive-interface <if-name> <if-address>
```

```
no passive-interface <if-name> <if-address>
```

模式

ospf 配置模式。

参数

if-name：接口名。

if-address：接口地址，32 位点分十进制形式。

描述

passive-interface 命令用来配置接口为被动接口，配置后接口能够收 ospf 报文，但不能发送 ospf 报文。

no passive-interface 命令用来恢复接口为可收发状态。

举例

#将接口 vlan55 配置为被动接口：

```
Switch(config-ospf-11)#passive-interface vlan55 172.20.10.1
```

```
Switch(config-ospf-11)#
```

10.1.35 redistribute

命令

```
redistribute <protocol> [metric <metric>] [metric-type <type>] [route-map  
<route-map>] [tag <tag>]
```

```
no redistribute <protocol> [metric <metric>] [metric-type <type>] [route-map  
<route-map>] [tag <tag>]
```

模式

ospf 配置模式。

参数

protocol:需要引入到 ospf 中的路由协议类型。

metric：指定引入路由的 metric 值。

type：引入的路由类型，取值为 1 或 2，缺省为 2。

route-map：引入路由时需要引用的 route-map 名。

tag：引入路由标记。

描述

redistribute 用来引入其他协议的路由到 ospf 中。

no redistribute 用来取消对其他协议路由的引入。缺省情况下不做路由引入。

举例

#引入直连路由到 ospf 路由表中，并通过 route-map 规则“list123”规则，指定引入路由的 metric 值为 9。

```
Switch(config-ospf-11)#redistribute connected metric 9 route-map list123
```

```
Switch(config-ospf-11)#
```

10.1.36 router ospf

命令

```
router ospf [<process-id>]  
no router ospf [<process-id>]
```

模式

全局配置模式。

参数

process-id : ospf 进程号，取值范围为 1 ~ 65535，缺省取值为 0。

描述

router ospf 命令用来创建 ospf 进程，并进入该进程的配置模式下。
no router ospf 命令用来删除一个 ospf 进程及该进程下的配置。

举例

```
#创建 ospf 进程 11 :  
Switch(config)#router ospf 11  
Switch(config-ospf-11)#
```

10.1.37 router-id

命令

```
router-id <router-id>  
no router-id [<router-id>]
```

模式

ospf 配置模式。

参数

router-id : 路由器 id，点分十进制格式。

描述

router-id 命令用来配置 ospf 进程的 router-id，系统在与邻居协商 ospf 时需要一个 AS 中惟一的身份标识。不配置时使用最大的接口 ip 地址作为 router-id。
no router-id 命令用来删除配置的 router-id，使用默认方式选择。

举例

```
#配置 ospf 进程使用 router-id 1.1.1.10 :
Switch(config-ospf-11)# router-id 1.1.1.10
Switch(config-ospf-11)#
```

10.1.38 summary-address

命令

```
summary-address <ip-prefix> [not-advertise] [tag <tag>]
no summary-address <ip-prefix> [not-advertise] [tag <tag>]
```

模式

ospf 配置模式。

参数

ip-prefix：需要聚合的路由范围，network/mask 形式。

not-advertise：聚合后不通告详细路由。

tag：指定聚合路由的 tag 值。

描述

summary-address 命令用来抑制或聚合外部引入的路由。从其他协议引入的路由，可以使用该命令聚合一定的范围。聚合后，在这个 prefix 覆盖范围内的路由将被抑制，只有聚合后的一条路由被广播。prefix 仅表示一个路由范围，引入的外部路由无需在这个范围内连续

no summary-address 命令用来删除配置的路由聚合。

举例

```
#配置 ospf 进程使用路由聚合：
Switch(config-ospf-11)#summary-address 1.1.0.0/20
Switch(config-ospf-11)#
```

10.1.39 timers spf

命令

```
timers spf <delay> <hold>
no timers spf <delay> <hold>
```

模式

ospf 配置模式。

参数

delay：延时时间，缺省为 5s。

hold：抑制时间，缺省为 10s。

描述

timers spf 命令用来配置 spf 计算计时器的延时时间和抑制时间。每次启动 spf 计算时，会计算上次 spf 计算到现在的抑制时间，若已经超过了配置的抑制时间则直接使用配置的延时时间启动计时器；若尚未超过配置的抑制时间，则使用配置的抑制时间计算出还需要延时的时间，若这个延时时间太小，小于配置的延时时间，则使用配置的延时时间，否则则使用计算出的延时时间启动计时器。

no timers spf 命令用来恢复 spf 计算定时器到默认值。

举例

#配置 ospf 进行 spf 计算的延时时间为 10s，抑制时间为 15s：

```
Switch(config-ospf-11)#timers spf 10 15
```

```
Switch(config-ospf-11)#
```

10.2 查看命令

10.2.1 show ip ospf

命令

```
show ip ospf [<process-id>]
```

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0~ 65535。

描述

show ip ospf 命令用来显示指定 ospf 进程相关的信息。不指定进程号时显示所有当前存在的进程的相关信息。

举例

#显示 ospf 进程 10 的相关信息：

```
Switch#show ip ospf 10
```

```
Routing Process "ospf 10" with ID 192.168.0.1
```

```
Process uptime is 1 day 7 hours 52 minutes
```

```
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 1. Checksum 0x007741
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 69
Number of LSA received 192
Number of areas attached to this router: 2
  Area 0 (BACKBONE)
    Number of interfaces in this area is 17(17)
    Number of fully adjacent neighbors in this area is 1
    Area has no authentication
    SPF algorithm last executed 31:09:58.285 ago
    SPF algorithm executed 10 times
    Number of LSA 5. Checksum 0x023ca6
  Area 1
    Number of interfaces in this area is 2(2)
    Number of fully adjacent neighbors in this area is 0
    Number of fully adjacent virtual neighbors through this area is 0
    Area has no authentication
    SPF algorithm last executed 31:52:10.025 ago
    SPF algorithm executed 4 times
    Number of LSA 20. Checksum 0x09f53d
```

Switch#

10.2.2 show ip ospf database

命令

```
show ip ospf [<process-id>] database [adv-router | asbr-summary | external  
| max-age | network | nssa-external | opaque-area | opaque-as |  
opaque-link | router | self-originate | summary]
```

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0~65535。

adv-router：通告路由链路状态信息。

asbr-summary：asbr 的 summary 链路状态信息。

external：外部路由链路状态信息。

max-age：age 列表中的链路状态信息。

network：Network 类型的链路状态信息。

nssa-external：NSSA 区域引入的链路状态信息。

opaque-area：Link area Opaque-LSA

router：路由器链路状态信息

self-originate：自己产生的链路状态信息。

summary：网络汇聚链路状态信息。

描述

show ip ospf [<process-id>] database 命令用来显示指定 ospf 进程的链路状态数据库信息。

举例

#显示 ospf 进程 10 的链路状态数据库中 networks 类型的信息：

```
Switch#show ip ospf 10 database network
```

```
OSPF Router with ID (192.168.0.1) (Process ID 10)
```

```
Net Link States (Area 0.0.0.0)
```

```
LS age: 531
```

```
Options: 0x22 (*|DC|E|)
```

```
LS Type: network-LSA
```

```
Link State ID: 172.20.5.3 (address of Designated Router)
```

```
Advertising Router: 192.168.130.2
```

```
LS Seq Number: 8000003e
```

```
Checksum: 0xe30a
```

Length: 32
Network Mask: /24
Attached Router: 192.168.130.2
Attached Router: 192.168.0.1

Switch#

10.2.3 show ip ospf interface

命令

show ip ospf interface [<if-name>]

模式

特权模式/普通模式。

参数

if-name : 需要显示 ospf 接口信息的接口名。

描述

show ip ospf interface 命令用来显示接口的 ospf 相关信息。

举例

#显示启动了 ospf 协议的接口的相关信息：

Switch# show ip ospf interface

vlan5 is up, line protocol is up

Internet Address 172.20.22.225/27, Area 0.0.0.1, MTU 1500

Process ID 10, Router ID 172.20.22.225, Network Type BROADCAST,

Cost: 10

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 172.20.22.225, Interface Address 172.20.22.225

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:07

Neighbor Count is 0, Adjacent neighbor count is 0

Crypt Sequence Number is 3774326953

Hello received 0 sent 5, DD received 0 sent 0

LS-Req received 0 sent 0, LS-Upd received 0 sent 0

LS-Ack received 0 sent 0, Discarded 0

vlan6 is down, line protocol is down

OSPF is enabled, but not running on this interface

```
vlan51 is up, line protocol is up
  Internet Address 172.20.6.2/24, Area 0.0.0.0, MTU 1500
  Process ID 10, Router ID 172.20.22.225, Network Type BROADCAST,
Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.20.22.225, Interface Address 172.20.6.2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 0, Adjacent neighbor count is 0
  Crypt Sequence Number is 3774326953
  Hello received 0 sent 5, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0

Switch#
```

10.2.4 show ip ospf neighbor

命令

```
show ip ospf [<process-id>] neighbor [<neighbor-id>] | [all | detail |
interface <if-address>]
```

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0~ 65535。

neighbor-id：邻居路由器 ID。

all：显示所有的邻居，包括 down 状态的。

detail：显示邻居的详细信息。

interface ifaddress：查看指定接口上的邻居信息。

描述

show ip ospf [<process-id>] neighbor 命令用来显示 ospf 的邻居信息。

举例

#显示 ospf 进程 10 的接口地址为 172.20.5.2 上的邻居信息：

```
Switch#show ip ospf nei inter 172.20.5.2
```



```
OSPF process 10
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.130.2	1	Full/DR	00:00:34	172.20.5.3	vlan10

```
Switch#
```

10.2.5 show ip ospf route

命令

```
show ip ospf [<process-id>] route [count]
```

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0~ 65535。

count：显示 ospf 路由条数。

描述

show ip ospf [process-id] route 命令用来显示 ospf 路由表。

举例

#显示 ospf 进程 10 的 ospf 路由条数：

```
Switch#show ip ospf 10 route coun
```

```
total routes: 21
```

```
Switch#
```

10.2.6 show ip ospf virtual-links

命令

```
show ip ospf [<process-id>] virtualLinks
```

模式

特权模式/普通模式。

参数

process-id：进程号，指定要查看的进程，取值范围 0~ 65535。

描述

show ip ospf [<process-id>] virtualLinks 命令用来查看虚连接的相关信息。

举例

#显示 ospf 进程 10 的 ospf 路由条数：

```
Switch#show ip ospf virtual-links
```

```
Virtual Link VLINK0 to router 1.1.1.10 is down
```

```
Transit area 0.0.0.1 via interface *
```

```
Local address *
```

```
Remote address *
```

```
Transmit Delay is 1 sec, State Down,
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
Hello due in inactive
```

```
Adjacency state Down
```

```
Switch#
```

10.2.7 show running ospf

命令

```
show running ospf
```

模式

特权模式/普通模式。

参数

无。

描述

show running ospf 命令用来查看当前系统中的 ospf 配置信息。

举例

#显示当前系统中 ospf 配置信息：

```
Switch#show running-config ospf
```

```
!
```

```
router ospf
```

```
!
```

```
router ospf 1
```

```
!
```

```
router ospf 10
```

```
network 172.20.5.0/24 area 0
```

```
network 172.20.6.0/24 area 0
```

```
network 172.20.7.0/24 area 0
```

```
network 172.20.11.0/24 area 0
```

```
network 172.20.22.192/27 area 1
network 172.20.22.224/27 area 1
area 1 virtual-link 1.1.1.10
!
router ospf 11
area 1 authentication message-digest
area 1 nssa default-information-originate no-summary
!
Switch#
```

10.3 调试命令

10.3.1 debug ospf

命令

```
debug ospf
no debug ospf
```

模式

特权模式。

参数

无。

描述

debug ospf 命令用来打开 ospf 相关调试开关，使用户能够看到 ospf 相关的协商过程和报文收发情况。

no debug ospf 命令用来关闭 ospf 调试开关

举例

#打开调试开关，显示 ospf 调试信息

```
Switch#debug ospf
```

```
Switch#
```

10.3.2 debug ospf all

命令

```
debug ospf all
```

no debug ospf all

模式

特权模式。

参数

无。

描述

debug ospf all 命令用来打开 ospf 相关的所有调试开关 使用户能够看到 ospf 相关的协商过程和报文收发情况。

no debug ospf all 命令用来关闭 ospf 相关的所有调试开关。

举例

#打开调试开关，显示出 ospf 所有调试信息

Switch#debug ospf all

Switch#

10.3.3 debug ospf events

命令

debug ospf events

no debug ospf events

模式

特权模式。

参数

无。

描述

debug ospf events 命令用来打开 ospf 事件调试开关，使用户能够看到 ospf 相关事件信息。

no debug ospf events 命令用来关闭 ospf 事件调试开关。

举例

#打开调试开关，显示 ospf 事件信息

Switch#debug ospf events

Switch#

10.3.4 debug ospf ifsm

命令

debug ospf ifsm
no debug ospf ifsm

模式

特权模式。

参数

无。

描述

debug ospf ifsm 命令用来打开 ospf 接口状态调试开关 ,使用户能够看到 ospf 接口状态机变迁信息。

no debug ospf ifsm 命令用来关闭接口状态机调试开关。

举例

#打开调试开关，显示出 ospf 接口状态变迁信息
Switch#debug ospf ifsm
Switch#

10.3.5 debug ospf lsa

命令

debug ospf lsa
no debug ospf lsa

模式

特权模式。

参数

无。

描述

debug ospf lsa 命令用来打开 ospf lsa 相关调试开关，使用户能够看到 lsa 收发信息。

no debug ospf lsa 命令用来关闭 ospf lsa 调试开关。

举例

#打开调试开关，显示出 ospf lsa 信息
Switch#debug ospf lsa
Switch#

10.3.6 debug ospf nfsm

命令

debug ospf nfsm
no debug ospf nfsm

模式

特权模式。

参数

无。

描述

debug ospf nfsm 命令用来打开 ospf 邻居状态调试开关,使用户能够看到 ospf 邻居状态变迁情况。

no debug ospf nfsm 命令用来关闭 ospf 邻居状态调试开关。

举例

#打开调试开关,显示 ospf 邻居状态变迁信息

Switch#debug ospf nfsm

Switch#

10.3.7 debug ospf packet

命令

debug ospf packet [recv | send] [detail]
no debug ospf packet [recv | send] [detail]

模式

特权模式。

参数

recv:接收报文信息。

send:发送报文信息。

detail:详细信息。

描述

debug ospf packet 命令用来打开 ospf 报文调试开关,使用户能够看到 ospf 报文的收发情况。

no debug ospf packet 命令用来关闭 ospf 报文调试开关。

举例

#打开调试开关，显示出 hello 报文的详细信息

```
Switch#debug ospf packet hello detail
```

```
Switch#
```

10.3.8 debug ospf route**命令**

```
debug ospf route
```

```
no debug ospf route
```

模式

特权模式。

参数

无。

描述

debug ospf route 命令用来打开 ospf 路由调试开关，使用户能够看到 ospf 路由调试信息。

no debug ospf route 命令用来关闭 ospf 路由调试开关。

举例

#打开调试开关，显示 ospf 路由调试信息

```
Switch#debug ospf route
```

```
Switch#
```

第 11 章 VRRP 命令

11.1 配置命令

11.1.1 disable/enable

命令

disable vrrp

enable vrrp

模式

vrrp 配置模式。

参数

无

描述

disable vrrp 命令用来禁止当前虚拟路由器的 vrrp 功能。

enable vrrp 命令用来使能当前虚拟路由器的 vrrp 功能。

举例

#使能 vlan10 下 id 为 10 的虚拟路由器的 vrrp 功能。

Switch(config)#router vrrp vlan10 10

Switch(config-vrrp)#enable vrrp

Switch(config-vrrp)

#禁止 vlan10 下 id 为 10 的虚拟路由器的 vrrp 功能。

Switch(config)#router vrrp vlan10 10

Switch(config-vrrp)#disable vrrp

Switch(config-vrrp)

11.1.2 router vrrp

命令

router vrrp <if-name> <vr-id>

no router vrrp <if-name> [<vr-id>]

模式

全局配置模式。

参数

if-name：接口名。

vr-id：虚拟路由器 ID，取值范围：1 ~ 255。

描述

router vrrp 命令用来使能一个接口 vrrp 功能，创建一个虚拟路由器并进入 vrrp 配置模式。

no router vrrp 命令用来删除一个 vrrp 虚拟路由器。

举例

#配置接口 vlan10 上使能 vrrp 功能，创建一个 ID 为 10 的虚拟路由器，并进入 vrrp 配置模式。

```
Switch(config)#router vrrp vlan10 10
```

```
Switch(config-vrrp)#
```

#删除接口 vlan10 上 ID 为 10 的虚拟路由器

```
Switch(config)#no router vrrp vlan10 10
```

```
Switch(config)#
```

11.1.3 vrrp ip-address

命令

```
vrrp ip-address <ip-address>
```

```
no vrrp ip-address
```

模式

vrrp 配置模式。

参数

ip-address：虚拟路由器的 ip 地址，点分十进制格式。

注：该地址必须与接口实际地址在同一网段。

描述

vrrp ip-address 命令用来为虚拟路由器配置 ip 地址。

no vrrp ip-address 命令用来删除虚拟路由器配置的 ip 地址。

举例

#配置 vlan10 下 ID 为 10 的虚拟路由器的虚拟 ip 地址为 192.168.1.1:

```
Switch(config)#router vrrp vlan10 10
```

```
Switch(config-vrrp)#vrrp ip-address 192.168.1.1
```

```
Switch(config-vrrp)
```

#删除 vlan10 下 ID 为 10 的虚拟路由器的虚拟 ip 地址

```
Switch(config)#router vrrp vlan10 10
Switch(config-vrrp)#no vrrp ip-address
Switch(config-vrrp)
```

11.1.4 vrrp advertisement-interval

命令

```
vrrp advertisement-interval <interval>
```

模式

vrrp 配置模式。

参数

interval：虚拟路由器发送周期性消息的时间间隔，单位为秒，取值范围：1~255。缺省为 1 秒。

描述

vrrp advertisement-interval 命令用来配置作为 master 的虚拟路由器发送周期性消息的时间间隔。

举例

```
#配置 vlan10 下 ID 为 10 的虚拟路由器周期性消息的时间间隔为 10 秒：
Switch(config)#router vrrp vlan10 10
Switch(config-vrrp)#vrrp advertisement-interval 10
Switch(config-vrrp)
```

11.1.5 vrrp authentication

命令

```
vrrp authentication {none | simple-password <password>}
```

模式

vrrp 配置模式。

参数

none：指定 vrrp 报文不使用验证。

simple-password <password>：指定 vrrp 使用简单文本验证，配置验证码。

描述

vrrp authentication 命令用来指定 vrrp 报文的验证方式和验证密码。

举例

#配置 vlan10 下 ID 为 10 的虚拟路由器使用简单文本验证，验证密码为 pass123：

```
Switch(config)#router vrrp vlan10 10
```

```
Switch(config-vrrp)#authentication simple-password pass123
```

```
Switch(config-vrrp)
```

11.1.6 vrrp preempt

命令

```
vrrp preempt {false | true}
```

模式

vrrp 配置模式。

参数

false：不使用抢占模式。

true：使用抢占模式。

描述

vrrp preempt 命令用来指定 vrrp 虚拟路由器是否使用抢占模式，当抢占模式为真时，同等情况下，使用抢占模式的一方将作为 master。缺省情况下为 true。

举例

#配置 vlan10 下 ID 为 10 的虚拟路由器不使用抢占模式：

```
Switch(config)#router vrrp vlan10 10
```

```
Switch(config-vrrp)#vrrp preempt false
```

```
Switch(config-vrrp)
```

11.1.7 vrrp priority

命令

```
vrrp priority <priority-number>
```

模式

vrrp 配置模式。

参数

priority-number：优先级值。取值范围为 3 ~ 254，1 ~ 2 为保留值，缺省为 100。

描述

vrrp priority 命令用来指定 vrrp 虚拟路由器发送协商报文的优先级。同等条件下，优先级高的一方成为 master。

举例

```
#配置 vlan10 下 ID 为 10 的虚拟路由器的优先级为 70 :
Switch(config)#router vrrp vlan10 10
Switch(config-vrrp)#vrrp priority 70
Switch(config-vrrp)
```

11.2 查看命令

11.2.1 show vrrp

命令

```
show vrrp [<if-name>]
```

模式

特权模式/普通模式。

参数

if-name：接口名。

描述

show vrrp 命令用来显示接口下当前已经配置的 vrrp 及其工作情况。缺省显示所有接口下的配置的所有 vrrp 信息。

举例

```
#查看 vlan10 接口下的 vrrp 配置 :
Switch#show vrrp vlan10
```

```
Vlan: 10 Vrid: 10
Virtual Router: Disabled
State: INITIALIZE
Virtual Ip Address:
Ip Address Owner: FALSE
Advertisement Interval: 10s
Protocol Priority: 100
Config Priority: 100
```

Preempt Mode: TRUE
Authentication Type: Simple Text Password
Authentication Password: pass123

Switch#

11.3 调试命令

11.3.1 debug vrrp

命令

debug vrrp
no debug vrrp

模式

特权模式。

参数

无。

描述

debug vrrp 命令用来打开当前 vrrp 的调试开关，使用户能够看到 vrrp 的协商过程和报文收发情况。

no debug vrrp 命令用来关闭 vrrp 的调试开关。

举例

#打开 vrrp 的调试开关：
Switch#debug vrrp
Switch#

11.3.2 debug vrrp all

命令

debug vrrp all
no debug vrrp all

模式

特权模式。

参数

无。

描述

debug vrrp all 命令用来打开所有 vrrp 相关的调试开关，使用户能够看到 vrrp 的协商过程和报文收发情况。

no debug vrrp all 命令用来关闭所有 vrrp 相关的调试开关。

举例

#打开 vrrp 相关的所有调试开关：

```
Switch#debug vrrp packet all
```

```
Switch#
```

11.3.3 debug vrrp events

命令

```
debug vrrp events
```

```
no debug vrrp events
```

模式

特权模式。

参数

无。

描述

debug vrrp events 命令用来打开 vrrp 的事件调试开关，使用户能够看到 vrrp 的协商过程。

no debug vrrp events 命令用来关闭 vrrp 的事件调试开关。

举例

#打开 vrrp 的事件信息调试开关：

```
Switch#debug vrrp events
```

```
Switch#
```

11.3.4 debug vrrp packet

命令

```
debug vrrp packet [recv | send] [detail]
```

```
no debug vrrp packet [recv | send] [detail]
```

模式

特权模式。

参数

recv：打开接收报文调试开关。

send：打开发送报文调试开关。

detail：打开 vrrp 报文的详细信息调试开关。

描述

debug vrrp 命令用来打开当前 vrrp 的调试开关，使用户能够看到 vrrp 的协商过程和报文收发情况。

no debug vrrp 命令用来关闭 vrrp 的调试开关。

举例

#打开 vrrp 的接收报文详细信息调试开关：

```
Switch#debug vrrp packet recv detail
```

```
Switch#
```

第 12 章 DHCP-RELAY 命令

12.1 配置命令

12.1.1 dhcp relay

命令

dhcp relay
no dhcp relay

模式

接口配置模式。

参数

无。

描述

dhcp relay 命令用来使能接口的 dhcp-relay 功能，缺省不使能接口的 dhcp-relay 功能。

no dhcp relay 命令用来关闭接口的 dhcp-relay 功能。

举例

#使能接口 vlan10 的 dhcp-relay 功能：

Switch(config-vlan10)#dhcp relay

Switch(config-vlan10)#

12.1.2 dhcp server

命令

dhcp server <ip-address>
no dhcp server <ip-address>

模式

接口配置模式。

参数

ip-address：DHCP 服务器的 ip 地址，点分十进制格式。

描述

dhcp server 命令用来指定一个 DHCP 服务器，交换机在收到 ip 地址请求报

文时将报文转发到指定的服务器请求地址（需启动 DHCP-Relay 功能）。该配置在入接口有效，即收到客户机 IP 地址请求的接口。

no dhcp server 命令用来删除接口上的 dhcp server 相关配置。

举例

#配置接口 vlan10 上请求 ip 地址的报文发向 DHCP 服务器：172.20.3.3：

```
Switch(config-vlan10)#dhcp relay
```

```
Switch(config-vlan10)# dhcp server 172.20.3.3
```

```
Switch(config-vlan10)#
```

12.2 查看命令

12.2.1 show debugging dhcp-relay

命令

```
show debugging dhcp-relay
```

模式

特权模式/普通模式。

参数

无

描述

show debugging dhcp-relay 命令用来查看当前的 dhcp-relay 调试开关的打开情况。

举例

#查看 dhcp-relay 的调试开关打开情况：

```
Switch#show debugging dhcp-relay
```

```
DHCP-relay debugging status:
```

```
  DHCPPr packet debugging is on
```

```
Switch#
```

12.3 调试命令

12.3.1 debug dhcp-relay

命令

debug dhcp-relay
no debug dhcp-relay

模式

特权模式。

参数

无。

描述

debug dhcp-relay 命令用来打开当前 dhcp-relay 的调试开关，使用户能够看到 dhcp-relay 的协商过程和报文收发情况。

no debug dhcp-relay 命令用来关闭 dhcp-relay 的调试开关。

举例

#打开 dhcp-relay 的调试开关：

```
Switch#debug dhcp-relay
Switch#
```

12.3.2 debug dhcp-relay all

命令

debug dhcp-relay all
no debug dhcp-relay all

模式

特权模式。

参数

无。

描述

debug dhcp-relay all 命令用来打开所有 dhcp-relay 相关的调试开关，使用户能够看到 dhcp-relay 的协商过程和报文收发情况。

no debug dhcp-relay all 命令用来关闭所有 dhcp-relay 相关的调试开关。

举例

#打开 dhcp-relay 相关的所有调试开关：

```
Switch#debug dhcp-relay packet all
```

```
Switch#
```

12.3.3 debug dhcp-relay events

命令

```
debug dhcp-relay events
```

```
no debug dhcp-relay events
```

模式

特权模式。

参数

无。

描述

debug dhcp-relay events 命令用来打开 dhcp-relay 的事件调试开关，使用户能够看到 dhcp-relay 的协商过程。

no debug dhcp-relay events 命令用来关闭 dhcp-relay 的事件调试开关。

举例

#打开 dhcp-relay 的事件信息调试开关：

```
Switch#debug dhcp-relay events
```

```
Switch#
```

12.3.4 debug dhcp-relay packet

命令

```
debug dhcp-relay packet [recv | send] [detail]
```

```
no debug dhcp-relay packet [recv | send] [detail]
```

模式

特权模式。

参数

recv：打开接收报文调试开关。

send：打开发送报文调试开关。

detail：打开 dhcp-relay 报文的详细信息调试开关。

描述

debug dhcp-relay packet 命令用来打开当前 dhcp-relay 的报文调试开关，使用户能够看到 dhcp-relay 报文的接收/发送情况。

no debug dhcp-relay packet 命令用来关闭 dhcp-relay 的报文调试开关。

举例

#打开 dhcp-relay 的接收报文详细信息调试开关：

```
Switch#debug dhcp-relay packet recv detail
```

```
Switch#
```

第 13 章 系统日志命令

13.1 通用日志命令

13.1.1 debug ip

命令

debug ip [all | arp | icmp | tcp | udp]

no debug ip [all | arp | icmp | tcp | udp]

模式

特权模式。

参数

all : 调试所有 ip、arp、icmp、udp、tcp 等协议包。解析 IP 包头的重要字段，包括协议类型、数据包长度和四层消息，如端口号等。

arp : 调试 arp 协议包，可以解析是 ARP 请求还是响应，可以解析 ARP 内容，发送端 IP 和接收端 MAC 地址信息等等。

icmp : 调试 icmp 协议数据报文的收发情况。该命令主要是通过解析包头的源和目的地址。

tcp : 调试运输层协议 TCP 的收发包情况，可以看到收发包窗口大小，应用层端口和报文大小以及源和目的地址。

udp : 调试运输层协议 udp 的收发包情况，可以看到应用层端口和报文大小以及收发包的源和目的地址。

描述

debug ip 命令用来打开以 ip 头封装的报文的相关调试开关，使用户能够看到指定类型的 ip 报文的报文收发情况。

no debug ip 命令关闭对应的 ip 报文调试开关。

举例

#打开 icmp 报文的调试开关：

```
Switch#debug ip icmp
```

```
Switch#
```

13.1.2 log display

命令

log display [critical | debugging | informational | warning]
no log display [critical | debugging | informational | warning]

模式

特权模式。

参数

critical : 输出 critical 级的信息。
debugging : 输出 debugging 级的调试信息。
informational : 输出法 information 级的调试信息。
warning : 输出 warning 级的调试信息。

举例

#输出所有打开调试开关调试信息：
Switch#log display
Switch#

13.1.3 no debug all

命令

no debug all

模式

特权模式。

参数

无。

描述

no debug all 命令用来关闭所有打开的调试开关。

举例

#关闭所有打开的调试开关：
Switch#no debug all
Switch#

13.1.4 show debugging

命令

show debugging [dhcp-relay | igmp | ip | mstp | ospf | rip | vrrp]

模式

特权模式/普通模式。

参数

dhcp-relay : dhcp-relay 的相关调试开关。

igmp : igmp 的相关调试开关。

ip : ip 的相关调试开关。

mstp : mstp 的相关调试开关。

ospf : ospf 的相关调试开关。

rip : rip 的相关调试开关。

vrrp : vrrp 的相关调试开关。

描述

show debug 命令用来查看当前打开了那些调试开关。

举例

#查看调试开关信息：

Switch#show debug

IP debugging status:

ICMP receive packets debugging is on.

ICMP send packets debugging is on.

RIP debugging status:

OSPF debugging status:

VRRP debugging status:

DHCP-relay debugging status:

MSTP debugging status:

IGMP SNOOPING debugging status:

Switch#

13.1.5 show log

命令

show log [critical | debugging | informational | warning]

模式

特权模式/普通模式。

参数

critical : 输出 critical 级的日志信息。

debugging : 输出 debugging 级的日志信息。

informational : 输出 informational 级的日志信息。

warning : 输出 warning 级的日志信息。

描述

show log 命令用来显示日志表中的日志信息。

举例

#显示 informational 级的日志信息：

Switch#show log informational

2089/08/10 11:01:24 Informational: ICMP: SEND: Destination IP:
172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0

2089/08/10 11:01:21 Informational: ICMP: SEND: Destination IP:
172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0

2089/08/10 11:01:18 Informational: ICMP: SEND: Destination IP:
172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0

2089/08/10 11:00:13 Informational: ICMP: SEND: Destination IP:
172.20.3.3 Source IP: 172.20.14.2 ICMP Type: 3 ICMP Code: 3

2089/08/10 11:00:13 Informational: ICMP: SEND: Destination IP:
172.20.3.3 Source IP: 172.20.14.2 ICMP Type: 3 ICMP Code: 3

2089/08/10 10:59:38 Informational: ICMP: SEND: Destination IP:
172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0

2089/08/10 10:53:21 Informational: ICMP: SEND: Destination IP:
172.20.3.3 Source IP: 172.20.10.2 ICMP Type: 3 ICMP Code: 3

Switch#

13.1.6 show log display

命令

show log display [critical | debugging | informational | warning]

模式

特权模式/普通模式。

参数

critical：输出严重级的日志信息。

debugging：输出调试信息。

informational：输出一般性提示级的日志信息。

warning：输出一般警告级的日志信息。

描述

show log display 命令用来显示四个优先级的终端实时监测开关的配置（打开还是关闭）。

举例

#显示监控配置信息：

Switch#show log display

Log display configuration:

Critical log: OFF

Warning log: OFF

Informational log: OFF

Debugging log: OFF

Switch#